

COMMUTING-LIFTABLE SUBGROUPS OF GALOIS GROUPS II

ADAM TOPAZ

ABSTRACT. Let n denote either a positive integer or ∞ , let ℓ be a fixed prime and let K be a field of characteristic different from ℓ . In the presence of sufficiently many roots of unity in K , we show how to recover some of the inertia/decomposition structure of valuations inside the maximal (\mathbb{Z}/ℓ^n) -abelian Galois group (resp. pro- ℓ abelian Galois group) of K using the maximal (\mathbb{Z}/ℓ^N) -abelian-by-central Galois group (resp. pro- ℓ -abelian-by-central Galois group) of K , whenever N is sufficiently large relative to n .

1. INTRODUCTION

The first key step in most strategies towards anabelian geometry is to develop a **local theory**, by which one recovers decomposition groups of “points” using the given Galois theoretic information. In the context of anabelian curves, one should eventually detect decomposition groups of closed points of the given curve within its étale fundamental group. On the other hand, in the birational setting, this corresponds to detecting decomposition groups of arithmetically and/or geometrically meaningful places of the function field under discussion within its absolute Galois group. The first instance of such a local theory is Neukirch’s group-theoretical characterization of decomposition groups of finite places of global fields;¹ indeed, this was the basis for the celebrated Neukirch-Uchida theorem [Neu69b], [Neu69], [Uch76]. The Neukirch-Uchida theorem was expanded by Pop to all higher dimensional finitely generated fields by developing a local theory based on his q -Lemma [Pop94], [Pop00]. The q -Lemma deals with the **absolute pro- q Galois theory**² of fields and, as with Neukirch’s result, works only in arithmetical situations.

On the other hand, at about the same time, two non-arithmetically based methods were proposed which recover inertia and decomposition groups of valuations from the **relative pro- ℓ Galois theory** (ℓ a fixed prime) of a field whose characteristic is different from ℓ . The first relies on the theory of **rigid elements** which was developed by several authors (see the details below). This theory requires only that the field under discussion has characteristic different from ℓ and that it contains μ_ℓ ; the input, however, must be the **maximal pro- ℓ Galois group** of the field (cf. [EN94], [Efr95], [EK98]). Nevertheless, this method eventually led to the characterization of solvable absolute Galois groups of fields by Koenigsmann [Koe01], and also the characterization of maximal pro- ℓ Galois groups of small rank [Koe98], [Efr98].

Date: October 8, 2012.

2010 Mathematics Subject Classification. 12E30, 12F10, 12G05, 12J25.

Key words and phrases. local theory, valuations, pro- ℓ Galois theory, Galois cohomology, abelian-by-central.

Research supported by a Benjamin Franklin fellowship from the University of Pennsylvania.

¹This actually predates Grothendieck’s anabelian geometry.

²Namely, fields whose absolute Galois group is a pro- q -group.

The second method is Bogomolov and Tschinkel's theory of **commuting-liftable pairs in Galois groups** [BT02].³ Its input is the much simpler **maximal pro- ℓ abelian-by-central Galois group**,⁴ but it requires that the base field contain an **algebraically closed subfield**. Nevertheless, this theory was a key technical tool in the local theory needed to settle Bogomolov's program in birational anabelian geometry for function fields over the algebraic closure of finite fields – see Bogomolov-Tschinkel [BT08] in dimension 2 and Pop [Pop12b] in general.

Until now, the two approaches – that of rigid elements versus that of commuting-liftable pairs – remained almost completely separate. However, Pop suggested in his Oberwolfach report [Pop06] that the two methods should be linked, even in the analogous (\mathbb{Z}/ℓ^n) -abelian-by-central situation, but unfortunately never followed up with the details. Also, the work done by Mahé, Mináč and Smith [MMS04] in the $(\mathbb{Z}/2)$ -abelian-by-central situation, and Efrat-Mináč [EM11] in special cases of the (\mathbb{Z}/ℓ) -abelian-by-central situation suggest a connection between the two methods in this analogous context.

This paper provides an approach which unifies the two methods. At the same time, we provide simpler arguments for the pro- ℓ abelian-by-central assertions of [BT02], and prove more general versions of these assertions which assume only that the field contains μ_{ℓ^∞} and not necessarily an algebraically closed subfield.⁵ The following Main Theorem is a summary of the more detailed Theorems 1 and 2.

Main Theorem. *Let $n \geq 1$ or $n = \infty$ be given, then for all $N \gg n$ the following holds. Let K be a field such that $\text{char } K \neq \ell$ which contains $\mu_{2\ell^N}$. Then there is a group-theoretical recipe which recovers (minimized) inertia and decomposition subgroups in the maximal \mathbb{Z}/ℓ^n -elementary-abelian Galois group of K using the group-theoretical structure encoded in the \mathbb{Z}/ℓ^N -abelian-by-central Galois group of K . Moreover, if $n = 1$ then $N = 1$ suffices and if $n \neq \infty$ then one can find (an explicit) $N \neq \infty$ as well.*

For readers' sake, we give a more detailed overview of the results mentioned above to see how the results of this paper fit into the larger context.

1.1. Overview. Let K be a field with $\text{char } K \neq \ell$ which contains the ℓ^{th} roots of unity $\mu_\ell \subset K$. Denote by $K(\ell)$ the maximal pro- ℓ Galois extension of K (inside a chosen separable closure of K) so that $\mathcal{G}_K := \text{Gal}(K(\ell)|K)$ is the maximal pro- ℓ quotient of the absolute Galois group G_K of K . Let w be a valuation of $K(\ell)$ and denote by $v = w|_K$ its restriction to K ; denote by $k(w)$ the residue field of w and $k(v)$ the residue field of v . We denote by $T_{w|v} \leq Z_{w|v} \leq \mathcal{G}_K$ the inertia resp. decomposition subgroup of $w|v$ inside \mathcal{G}_K . Recall that $Z_{w|v}/T_{w|v} = \mathcal{G}_{k(v)}$ and that the canonical short exact sequence

$$1 \rightarrow T_{w|v} \rightarrow Z_{w|v} \rightarrow \mathcal{G}_{k(v)} \rightarrow 1$$

is split. Moreover, if $\text{char } k(v) \neq \ell$, then $T_{w|v}$ is a free abelian pro- ℓ group of the same rank as $v(K^\times)/\ell$, and the action of $\mathcal{G}_{k(v)}$ on $T_{w|v}$ factors via the ℓ -adic cyclotomic character. Thus,

³This theory was originally proposed by Bogomolov [Bog91].

⁴Terminology by Pop [Pop10b].

⁵Compare with [BT02] where the existence of an algebraically closed subfield is essential in the proof.

if $\text{char } k(v) \neq \ell$, and $\sigma \in T_{w|v}$, $\tau \in Z_{w|v}$ are given non-torsion elements so that the closed subgroup $\langle \sigma, \tau \rangle$ ⁶ is non-pro-cyclic, then $\langle \sigma, \tau \rangle = \langle \sigma \rangle \rtimes \langle \tau \rangle \cong \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell$ is a semi-direct product.

In a few words, the theory of rigid elements in the context of pro- ℓ Galois groups [EN94], [Efr95], [EK98] asserts that the only way the situation above can arise is from valuation theory, as described above. More precisely, let K be a field such that $\text{char } K \neq \ell$ and $\mu_\ell \subset K$. If $\sigma, \tau \in \mathcal{G}_K$ are non-torsion elements such that $\langle \sigma, \tau \rangle = \langle \sigma \rangle \rtimes \langle \tau \rangle$ is non-pro-cyclic, then there exists a valuation w of $K(\ell)$ such that, denoting $v = w|_K$, one has $\text{char } k(v) \neq \ell$, $v(K^\times) \neq v(K^{\times \ell})$, $\sigma, \tau \in Z_{w|v}$ and $\langle \sigma, \tau \rangle / \langle \sigma, \tau \rangle \cap T_{w|v}$ is cyclic. The key technique in this situation is the explicit “creation” of valuation rings inside K using rigid elements and so-called “ ℓ -rigid calculus” developed, for instance, in [Koe95] and/or [Efr99]. Indeed, under the assumption that $\mathcal{G}_K = \langle \sigma, \tau \rangle = \langle \sigma \rangle \rtimes \langle \tau \rangle$ as above, one shows that K has sufficiently many “strongly-rigid elements” to produce an ℓ -Henselian valuation v of K with $v(K^\times) \neq v(K^{\times \ell})$ and $\text{char } k(v) \neq \ell$. Rigid elements were first considered by Ware [War81], then further developed in the context of valuation theory and/or Galois theory by Arason-Elman-Jacob in [AEJ87], Engler-Nogueria in [EN94], Koenigsmann in [Koe95], Engler-Koenigsmann in [EK98], Efrat in [Efr95], [Efr99], [Efr07] and also by others.

Assume, on the other hand, that $\mu_{\ell^\infty} \subset K$. In this case, we denote by

$$\Pi_K^a := \frac{\mathcal{G}_K}{[\mathcal{G}_K, \mathcal{G}_K]}, \quad \text{and} \quad \Pi_K^c := \frac{\mathcal{G}_K}{[\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]]}$$

the maximal pro- ℓ abelian resp. maximal pro- ℓ abelian-by-central Galois groups of K – this terminology and notation was introduced by Pop [Pop10b]. In the above context, assume again that $\text{char } k(v) \neq \ell$, then the ℓ -adic cyclotomic character of K (and of $k(v)$) is trivial. Hence, $\mathcal{G}_{k(v)}$ acts trivially on $T_{w|v}$; we conclude that $Z_{w|v} \cong T_{w|v} \times \mathcal{G}_{k(v)}$ and recall that $T_{w|v}$ is abelian. Denote by K^{ab} the Galois extension of K such that $\text{Gal}(K^{ab}|K) = \Pi_K^a$, $v^{ab} := w|_{K^{ab}}$, $T_v := T_{v^{ab}|v}$ and $Z_v := Z_{v^{ab}|v}$; since Π_K^a is abelian, T_v and Z_v are independent of choice of w . We deduce that for all $\sigma \in T_v$ and $\tau \in Z_v$, there exist lifts $\tilde{\sigma}, \tilde{\tau} \in \Pi_K^c$ of $\sigma, \tau \in \Pi_K^a$ which commute in Π_K^c ; since Π_K^c is a central extension of Π_K^a , we conclude that **any lifts** $\tilde{\sigma}, \tilde{\tau} \in \Pi_K^c$ of $\sigma, \tau \in \Pi_K^a$ commute as well – such a pair $\sigma, \tau \in \Pi_K^a$ is called **commuting-liftable**.

Bogomolov and Tschinkel’s theory of commuting-liftable pairs [BT02] asserts that, under the assumption that K contains an algebraically closed subfield $k = \bar{k}$, the only way a commuting pair can arise is via a valuation as described above.⁷ The method of loc.cit. uses the notion of a “flag function;” in particular, this is a homomorphism $K^\times \rightarrow \mathbb{Z}_\ell$ which corresponds, via Kummer theory, to an element in T_v for some valuation v .⁸ One then considers σ, τ as elements of $\text{Hom}(K^\times, \mathbb{Z}_\ell) = \text{Hom}(K^\times/k^\times, \mathbb{Z}_\ell)$ via Kummer theory, and produces the corresponding map:

$$\Psi = (\sigma, \tau) : K^\times/k^\times \rightarrow \mathbb{Z}_\ell^2 \subset \mathbb{A}^2(\mathbb{Q}_\ell).$$

When one views $K^\times/k^\times = \mathbb{P}_k(K)$ as an infinite dimensional projective space over k , the assumption that σ, τ are commuting liftable ensures that Ψ sends **projective lines** to **affine**

⁶We denote by $\langle S \rangle$ the closed subgroup generated by S .

⁷It turns out that $\text{char } k(v) \neq \ell$ is not needed in order to produce a commuting-liftable pair, under a modified notion of decomposition and inertia. It turns out that valuations with residue characteristic equal to ℓ can and do arise from commuting-liftable pairs, as we will see in this paper.

⁸We generalize the notion of a flag function in this paper.

lines. This severe restriction on Ψ is then used to show that some \mathbb{Z}_ℓ -linear combination of σ and τ is a flag function.

As mentioned above, the theory of commuting-liftable pairs was originally outlined by Bogomolov in [Bog91], where he also introduced a program in birational anabelian geometry for fields of purely geometric nature – i.e. function fields over an algebraically closed field of characteristic different from ℓ and dimension ≥ 2 – which aims to reconstruct such function fields K from the Galois group Π_K^c . If $\text{char } K > 0$, the above technical theorem eventually allows one to detect the decomposition and inertia subgroups of **quasi-divisorial valuations** inside Π_K^a using the group-theoretical structure encoded in Π_K^c (see Pop [Pop10b]). In particular, for function fields K over the algebraic closure of a finite field, one can detect the decomposition/inertia structure of **divisorial valuations** inside Π_K^a using Π_K^c . While Bogomolov’s program in its full generality is far from being complete, it has been carried through for function fields $K|k$, $k = \overline{\mathbb{F}}_p$ over the algebraic closure of a finite field – by Bogomolov-Tschinkel [BT08] in dimension 2, and by Pop [Pop12b] in general.

In this paper, we obtain analogous results to those in the theory of commuting-liftable pairs, for the (\mathbb{Z}/ℓ^n) -abelian-by-central and the pro- ℓ -abelian-by-central situations, by elaborating on and using the theory of rigid elements, while working under less restrictive assumptions than Bogomolov and Tschinkel’s approach. In particular, we reprove and generalize the main results of [BT02] using this method. We begin by introducing some technical assumptions and notation.

1.2. Notation. For the remainder of the paper, ℓ will denote a fixed prime. A “subgroup” in the context of profinite groups will always mean a closed subgroup, and all homomorphisms we consider will be continuous. For an abelian group A , we will denote by \widehat{A} the ℓ -adic completion of A ; namely:

$$\widehat{A} := \lim_n A/\ell^n.$$

To simplify the notation somewhat, for a field F we will denote by $\widehat{F} = \widehat{F^\times}$, the ℓ -adic completion of F^\times .

Let K be a field whose characteristic is different from ℓ . Let n denote either a positive integer or $n = \infty$ and assume that $\mu_{2\ell^n} \subset K$. In this case, we denote by $\mathcal{G}_K^{a,n}$ the maximal (\mathbb{Z}/ℓ^n) -abelian (resp. pro- ℓ abelian if $n = \infty$) and $\mathcal{G}_K^{c,n}$ the maximal (\mathbb{Z}/ℓ^n) -abelian-by-central (resp. pro- ℓ -abelian-by-central) Galois groups of K . Explicitly, denote by $\mathcal{G}_K^{(2,n)} := [\mathcal{G}_K, \mathcal{G}_K] \cdot (\mathcal{G}_K)^{\ell^n}$ and $\mathcal{G}_K^{(3,n)} = [\mathcal{G}_K, \mathcal{G}_K^{(2,n)}] \cdot (\mathcal{G}_K^{(2,n)})^{\ell^n}$, then

$$\mathcal{G}_K^{a,n} := \mathcal{G}_K / \mathcal{G}_K^{(2,n)}, \quad \text{and} \quad \mathcal{G}_K^{c,n} := \mathcal{G}_K / \mathcal{G}_K^{(3,n)}.$$

The canonical projection $\Pi : \mathcal{G}_K^{c,n} \twoheadrightarrow \mathcal{G}_K^{a,n}$ induces the following maps; we denote $\ker \Pi$ additively. First, $[\bullet, \bullet] : \mathcal{G}_K^{a,n} \times \mathcal{G}_K^{a,n} \rightarrow \ker \Pi$ defined by $[\sigma, \tau] = \tilde{\sigma}^{-1} \tilde{\tau}^{-1} \tilde{\sigma} \tilde{\tau}$ where $\tilde{\sigma}, \tilde{\tau} \in \mathcal{G}_K^{c,n}$ are some lifts of $\sigma, \tau \in \mathcal{G}_K^{a,n}$; since Π is a central extension, this is well-defined and bilinear. Second, $(\bullet)^\pi : \mathcal{G}_K^{a,n} \rightarrow \ker \Pi$ defined by $\sigma^\pi = \tilde{\sigma}^{\ell^n}$ (resp. $\sigma^\pi = 0$ if $n = \infty$) where, again, $\tilde{\sigma} \in \mathcal{G}_K^{c,n}$ is some lift of $\sigma \in \mathcal{G}_K^{a,n}$; since Π is a central extension with kernel killed by ℓ^n , this map is well defined and, if $\ell \neq 2$, this map is linear. We will furthermore denote by $\sigma^\beta = 2 \cdot \sigma^\pi$ – thus $(\bullet)^\beta$ is a linear map $\mathcal{G}_K^{a,n} \rightarrow \ker \Pi$ regardless of ℓ .

A pair of elements $\sigma, \tau \in \mathcal{G}_K^{a,n}$ will be called a **commuting-liftable** pair (or a **CL-pair** for short) provided that $[\sigma, \tau] \in \langle \sigma^\beta, \tau^\beta \rangle$. For a (closed) subgroup $A \leq \mathcal{G}_K^{a,n}$, we denote by

$$\mathbf{I}^{\text{CL}}(A) = \{\sigma \in A : \forall \tau \in A, [\sigma, \tau] \in \langle \sigma^\beta, \tau^\beta \rangle\}.$$

Then $\mathbf{I}^{\text{CL}}(A)$ is a subgroup⁹ of A – this is the so-called “commuting-liftable-center” of A .

Remark 1.1. Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{2\ell} \subset K$, and let $A \leq \mathcal{G}_K^{a,1}$ be given. In this case, we can give an alternative definition for $\mathbf{I}^{\text{CL}}(A)$ which is the same definition given in [Top12]. Namely, for $A \leq \mathcal{G}_K^{a,1}$ one has $\mathbf{I}^{\text{CL}}(A) = \{\sigma \in A : \forall \tau \in A, [\sigma, \tau] \in A^\beta\}$. See Remark 7.6 for the proof of this equivalence.

Suppose v is a valuation of K . We will denote by $\Gamma_v = v(K^\times)$ the value group, \mathcal{O}_v the valuation ring with valuation ideal \mathfrak{m}_v , and $k(v) = \mathcal{O}_v/\mathfrak{m}_v$ the residue field of v . We denote by $K^{a,n} = K(\sqrt[n]{K})$ the Galois extension of K such that $\text{Gal}(K^{a,n}|K) = \mathcal{G}_K^{a,n}$, and pick a prolongation v' of v to $K^{a,n}$. We denote by $T_v^n := T_{v'|v}$ and $Z_v^n = Z_{v'|v}$ the decomposition and inertia subgroups of $v'|v$ inside $\mathcal{G}_K^{a,n}$; since $\mathcal{G}_K^{a,n}$ is abelian, these groups are independent of choice of v' . Moreover, we introduce the **minimized** decomposition and inertia subgroups:

$$D_v^n := \text{Gal}(K^{a,n}|K(\sqrt[n]{1 + \mathfrak{m}_v})), \quad \text{and} \quad I_v^n := \text{Gal}(K^{a,n}|K(\sqrt[n]{\mathcal{O}_v^\times})).$$

Observe that $I_v^n \leq D_v^n$; more importantly, however, $I_v^n \leq T_v^n$ and $D_v^n \leq Z_v^n$ with equality whenever $\text{char } k(v) \neq \ell$ (see Proposition 9.1). It turns out that the minimized inertia and decomposition groups, $I_v^n \leq D_v^n$, have an abelian-by-central Galois theoretical structure which resembles that of the usual inertia and decomposition, even for valuations whose residue characteristic is ℓ – see Remark 7.7 for the details. In particular, for any valuation v of K , one has $I_v^n \leq \mathbf{I}^{\text{CL}}(D_v^n)$ just as $T_v^n \leq \mathbf{I}^{\text{CL}}(Z_v^n)$ which can be deduced from the discussion above.

We denote by $\mathcal{W}_{K,n}$ the collection of valuations v of K which satisfy the following conditions:

- (1) Γ_v contains no non-trivial ℓ -divisible convex subgroups.
- (2) v is maximal among all valuations w such that $D_v^n = D_w^n$ and Γ_w contains no non-trivial ℓ -divisible convex subgroups; i.e. for all refinements w of v such that $D_w^n = D_v^n$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I_w^n = I_v^n$.

Furthermore, denote by $\mathcal{V}_{K,n}$ the subset of valuations $v \in \mathcal{W}_{K,n}$ such that $k(v)^\times/\ell^n$ (resp. $\widehat{k(v)}$ if $n = \infty$) is non-cyclic. It turns out that many valuations of interest are contained in $\mathcal{W}_{K,n}$. For instance, if K is a function field over an algebraically closed field k , then all Parshin chains of divisors are contained in $\mathcal{W}_{K,n}$ and those Parshin chains of non-maximal length are contained in $\mathcal{V}_{K,n}$ (this is also true when k is a “strongly” ℓ -closed field – see Example 4.3).

In a similar way, we will denote by $\mathcal{V}'_{K,n}$ the collection of valuations v of K which satisfy the following conditions:

- (1) $\text{char } k(v) \neq \ell$.
- (2) Γ_v contains no non-trivial ℓ -divisible convex subgroups.

⁹This is not immediate if $n \neq \infty$, but follows from Theorem 11. See also Remark 1.1 and/or 7.6 for the case $n = 1$. See also Remark 7.7 alongside the main results of the paper to see that this definition of \mathbf{I}^{CL} is indeed sufficient in the context of valuation theory.

- (3) v is maximal among all valuations w such that $\text{char } k(w) \neq \ell$, $D_v^n = D_w^n$ and Γ_w contains no non-trivial ℓ -divisible convex subgroups; i.e. for all refinements w of v such that $\text{char } k(w) \neq \ell$ and $D_w^n = D_v^n$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I_w^n = I_v^n$.
- (4) $\mathcal{G}_{k(v)}^{a,n}$ is non-cyclic.

Observe that the collection of all valuations $v \in \mathcal{V}_{K,n}$ whose residue characteristic is different from ℓ lies in $\mathcal{V}'_{K,n}$; in general, however, the two sets are quite different. Moreover, note that $\mathcal{V}_{K,n} = \mathcal{V}'_{K,n}$ provided that $\text{char } K > 0$.

Remark 1.2. Using the results of this paper, we can give an alternative equivalent definition for $\mathcal{V}_{K,n}$ in the case where $\text{char } K \neq \ell$ and $\mu_{2\ell^n} \subset K$ which is much more natural, as follows – see Lemma 4.8 and Theorem 11. $\mathcal{V}_{K,n}$ is precisely the collection of valuations v of K such that:

- (1) Γ_v contains no non-trivial ℓ -divisible convex subgroups.
- (2) $I_v^1 = \mathbf{I}^{\text{CL}}(D_v^1) \neq D_v^1$.

In particular, we see that $\mathcal{V}_{K,m} = \mathcal{V}_{K,n}$ for all $m \leq n$.

Denote by \mathbb{N} the collection of positive integers and $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$; we declare that $\infty > n$ for all $n \in \mathbb{N}$. If $N \geq n$ and $\mu_{\ell^N} \subset K$, we will denote the canonical map $\mathcal{G}_K^{a,N} \rightarrow \mathcal{G}_K^{a,n}$ by $f \mapsto f_n$. Furthermore, for an extension $L|K$ of fields, we will denote by $f \mapsto f_K$ the canonical map $\mathcal{G}_L^{a,n} \rightarrow \mathcal{G}_K^{a,n}$.

1.3. Main Results of the Paper. The main goal of this paper is to produce a function $\mathbf{R} : \overline{\mathbb{N}} \rightarrow \overline{\mathbb{N}}$, satisfying the following conditions:

- If $n \in \mathbb{N}$ then $\mathbf{R}(n) \in \mathbb{N}$.
- $\mathbf{R}(1) = 1$ and $\mathbf{R}(\infty) = \infty$.
- $\mathbf{R}(n) \geq n$ for all $n \in \overline{\mathbb{N}}$.

such that Theorems 1 and 2 hold. While we succeed to construct such a function \mathbf{R} (in the notation introduced in Part 1, $\mathbf{R}(n) = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$ suffices), we do not expect that our function is optimal. However, the requirement that $\mathbf{R}(1) = 1$ and $\mathbf{R}(\infty) = \infty$ ensures that Theorems 1 and 2 include the main results of [Top12] and therefore also [BT02] as special cases. See also Theorem 2 parts (1) and (2) along with Remark 1.1 in comparison with the main theorems of [EN94], [Efr95], [EK98], and also the main theorem of [EM11].

Theorem 1. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{R}(n)$. Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{2\ell^N} \subset K$.*

- (1) *Let $D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation v of K such that $D \leq D_v^n$ and $D/D \cap I_v^n$ is cyclic if and only if there exists a CL-group $D' \leq \mathcal{G}_K^{a,N}$ such that $D'_n = D$.*
- (2) *Let $I \leq D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v^n$ and $D = D_v^n$ if and only if the following hold:*
 - (a) *There exist $D' \leq \mathcal{G}_K^{a,N}$ such that $(\mathbf{I}^{\text{CL}}(D'))_n = I$ and $D'_n = D$.*
 - (b) *$I \leq D \leq \mathcal{G}_K^{a,n}$ are maximal with this property – i.e. if $D \leq E \leq \mathcal{G}_K^{a,n}$ and $E' \leq \mathcal{G}_K^{a,N}$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^{\text{CL}}(E'))_n$, then $D = E$ and $I = (\mathbf{I}^{\text{CL}}(E'))_n$.*
 - (c) *$\mathbf{I}^{\text{CL}}(D) \neq D$ (i.e. D is not a CL-group).*

In particular, Theorem 1 part 2 provides a group theoretical recipe to detect $I_v^n \leq D_v^n$ for $v \in \mathcal{V}_{K,n}$ using only the group-theoretical structure of $\mathcal{G}_K^{c,N}$, whenever $\mu_{2\ell^N} \subset K$ where $N = \mathbf{R}(n)$ as in the theorem.

By enlarging the group $\mathcal{G}_K^{c,N}$ we can detect which of those valuations v in the theorem above have residue characteristic different from ℓ . This therefore gives a group-theoretical recipe to detect decomposition and inertia subgroups of valuations $v \in \mathcal{V}_{K,n}$ whose residue characteristic is different from ℓ .

Theorem 2. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{R}(n)$. Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{2\ell^N} \subset K$.*

- (1) *Let $D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L = (K^{a,n})^D$. Then there exists a valuation v of K such that $\text{char } k(v) \neq \ell$, $D \leq Z_v^n$ and $D/D \cap T_v^n$ is cyclic if and only if there exists a CL-group $D' \leq \mathcal{G}_L^{a,N}$ such that $(D'_n)_K = D$.*
 - (2) *Assume that $\mathbf{I}^{\text{CL}}(\mathcal{G}_K^{a,n}) \neq \mathcal{G}_K^{a,n}$ and consider $(\mathbf{I}^{\text{CL}}(\mathcal{G}_K^{a,N}))_n =: T$. Then there exists a (possibly trivial) valuation $v \in \mathcal{V}_{K,n}$ such that $\text{char } k(v) \neq \ell$, $T = T_v^n$ and $\mathcal{G}_K^{a,n} = Z_v^n$.*
 - (3) *Let $v \in \mathcal{V}_{K,n}$ be given and denote by $I := I_v^n \leq D_v^n =: D$, $L = (K^{a,n})^D$. Then $\text{char } k(v) \neq \ell$ if and only if there exist $I' \leq D' \leq \mathcal{G}_L^{a,N}$ such that:*
 - (a) $I' \leq \mathbf{I}^{\text{CL}}(D')$.
 - (b) $(I'_n)_K = I$ and $(D'_n)_K = D$.
- Moreover, if these equivalent conditions hold then $I = I_v^n = T_v^n$ and $D = D_v^n = Z_v^n$.*
- (4) *Let $I \leq D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L = (K^{a,n})^D$. Then there exists a valuation $v \in \mathcal{V}'_{K,n}$ such that $I = T_v^n$ and $D = Z_v^n$ if and only if the following hold:*
 - (a) *There exist $D' \leq \mathcal{G}_L^{a,N}$ such that $(\mathbf{I}^{\text{CL}}(D'))_n = I$ and $(D'_n)_K = D$.*
 - (b) *$I \leq D \leq \mathcal{G}_K^{a,n}$ are maximal with this property – i.e. if $D \leq E \leq \mathcal{G}_K^{a,n}$ and $E' \leq \mathcal{G}_L^{a,N}$ is given such that $(E'_n)_K = E$ and $I \leq (\mathbf{I}^{\text{CL}}(E'))_n$, then $D = E$ and $I = (\mathbf{I}^{\text{CL}}(E'))_n$.*
 - (c) $\mathbf{I}^{\text{CL}}(D) \neq D$ (i.e. D is not a CL-group).

Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{R}(n)$. Denote by $\mathcal{G}_K^{M,n}$ the smallest quotient of \mathcal{G}_K for which $\mathcal{G}_L^{c,N}$ is a subquotient for all $K \subset L \subset K^{a,n}$. Therefore, Theorem 1 part 2 along with Theorem 2 part 3 provide a group-theoretical recipe to detect $T_v^n \leq Z_v^n$ for valuations $v \in \mathcal{V}_{K,n}$ such that $\text{char } k(v) \neq \ell$, using only the group-theoretical structure of $\mathcal{G}_K^{M,n}$. Moreover, part 4 of this theorem provides a group-theoretical recipe to detect $T_v^n \leq Z_v^n$ for valuations $v \in \mathcal{V}'_{K,n}$ using only the group-theoretical structure of $\mathcal{G}_K^{M,n}$.

1.4. A Guide Through the Paper. In Part 1, we develop the underlying theory which proves the main results of the paper. This theory works for an arbitrary field K , and is based on an abstract notion of “C-pairs” which is related to a condition in the Milnor K-theory of the field (see Proposition 6.1). Thus, we show how to detect valuations using the Milnor K-theory of a field (see Remark 6.3) without the presence of any Galois theory.

In Part 2, we provide this K-theoretic condition which detects C-pairs. On the other hand, the main theorem of Part 2, Theorem 11, shows that the two notions – that of C-pairs and that of CL-pairs – are identical in the situation where $\text{char } K \neq \ell$ and $\mu_{2\ell^N} \subset K$. Using this theorem, Theorem 1 is a mere translations to the results from the abstract situation considered in Part 1.

In part 3, we provide the applications of this theory and, for example, show Theorem 2. We also prove the following corollary which provides a sufficient condition to detect whether or not $\text{char } K = 0$ using the Galois group $\mathcal{G}_K^{M,n}$:

Corollary 1.3. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{R}(n)$. Let K be a field such that $\text{char } K = 0$ and $\mu_{2\ell^N} \subset K$. Assume that there exists a field F such that $\text{char } F > 0$, $\mu_{2\ell^N} \subset F$ and $\mathcal{G}_K^{M,n} \cong \mathcal{G}_F^{M,n}$. Then for all $v \in \mathcal{V}_{K,n}$ one has $\text{char } k(v) \neq \ell$.*

As a consequence of this, we find many examples of fields K of characteristic 0 whose maximal pro- ℓ Galois group \mathcal{G}_K is not isomorphic to \mathcal{G}_F for any field F of positive characteristic.

Corollary 1.4. *Suppose that K is one of the following:*

- *A function field over a global field k of characteristic 0 such that $\mu_{2\ell} \subset k$, and $\dim(K|k) \geq 1$.*
- *A function field over a strongly ℓ -closed¹⁰ field k (e.g. k an algebraically closed field) of characteristic 0 such that $\dim(K|k) \geq 2$.*

Then there does not exist a field F such that $\mu_{2\ell} \subset F$, $\text{char } F > 0$ and $\mathcal{G}_K \cong \mathcal{G}_F$.

Acknowledgments. The author would like to thank all who expressed interest in this work and in particular Florian Pop, Jakob Stix, Jochen Koenigsmann, Moshe Jarden, Dan Haran, Lior Bary-Soroker and Ján Mináč.

Part 1. Underlying Theory

In the first part of this paper, we develop the underlying theory using an abstract notion of “C-pairs.” It turns out, as we will see in Part 2, that this notion is equivalent to that of CL-pairs as defined in the introduction. Throughout, we will tacitly use the following trivial observation and dub it “the Cancellation Principle:”

Lemma 1.5 (The Cancellation Principle). *For a positive integer n , we denote by $\mathbf{M}_r(n) = (r+1) \cdot n - r$. Assume that $R \geq (r+1) \cdot n - r = \mathbf{M}_r(n)$. Let $a, b, c_1, \dots, c_r \in \mathbb{Z}/\ell^R$ be given; assume that $c_i \not\equiv 0 \pmod{\ell^n}$ and that $ac_1 \cdots c_r = bc_1 \cdots c_r$. Then $a = b \pmod{\ell^n}$.*

Proof. Let a be the minimal positive integer such that $\ell^a \cdot c_1 \cdots c_r = 0$ as an element of \mathbb{Z}/ℓ^R . Then the map $\mathbb{Z}/\ell^a \rightarrow \mathbb{Z}/\ell^R$ defined by $x \mapsto x \cdot c_1 \cdots c_r$ is injective. On the other hand, as $c_i \not\equiv 0 \pmod{\ell^n}$, we observe that $a \geq R - rn + r \geq n$ and this proves the claim. \square

2. MAIN THEOREM OF C-PAIRS

We denote by $\mathbb{N} = \{1, 2, 3, \dots\}$ the set of positive integers and $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ the set of positive integers together with ∞ . We declare that $\infty > n$ for all $n \in \mathbb{N}$.

For positive integers n and r , we denote by

$$\mathbf{M}_r(n) = (r+1) \cdot n - r, \quad \mathbf{N}'(n) = (6\ell^{3n-2} - 7) \cdot (n-1) + 3n - 2, \quad \mathbf{N}(n) = \mathbf{M}_1(\mathbf{N}'(n)).$$

To make the notation consistent, we denote by $\mathbf{M}_r(\infty) = \mathbf{N}(\infty) = \infty$. In particular, $\mathbf{N}(n) \geq \mathbf{M}_1(n) \geq n$ for all $n \in \overline{\mathbb{N}}$, and $\mathbf{N}(n), \mathbf{M}_r(n) \in \mathbb{N}$ if and only if $n \in \mathbb{N}$. Also, observe that $\mathbf{M}_r(1) = \mathbf{N}'(1) = \mathbf{N}(1) = 1$, and $\mathbf{M}_r(\infty) = \mathbf{N}'(\infty) = \mathbf{N}(\infty) = \infty$.

¹⁰See Example 4.3 for the definition of a strongly ℓ -closed field.

We will use the following notation:

$$R_n := \lim_{m|n} \mathbb{Z}/\ell^m = \begin{cases} \mathbb{Z}/\ell^n, & n \in \mathbb{N} \\ \mathbb{Z}_\ell, & n = \infty \end{cases}$$

In the context of pro- ℓ Galois theory, we will also denote by $R_n(m) = R_n \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(m)$ the m^{th} Tate twist of R_n ; this notation will not be needed until Part 2.

Let M be an R_n -module. A collection of non-zero elements $(f_i)_i$, $f_i \in M$ will be called **quasi-independent** provided that

$$\sum_i a_i f_i = 0 \text{ almost all } a_i = 0 \Rightarrow a_i f_i = 0 \forall i.$$

A generating set which is quasi-independent will be called a quasi-basis. Observe that any finitely generated R_n module M has a quasi-basis of unique finite order which is equal to $\dim_{\mathbb{Z}/\ell}(M/\ell)$. Indeed, any finitely generated R_n module M can be written as a direct product of cyclic submodules:

$$M = \prod_{i=1}^n \langle \sigma_i \rangle$$

and in this case $(\sigma_i)_i$ form a quasi-basis for M .

Let K be a field and $n \in \overline{\mathbb{N}}$. We denote by:

$$\mathcal{G}_K^a(n) := \text{Hom}(K^\times / \pm 1, R_n);$$

endowed with the point-wise convergence topology, we consider $\mathcal{G}_K^a(n)$ as a pro- ℓ Group.

For $n, N \in \mathbb{N}$, $N \geq n$ and $f \in \mathcal{G}_K^a(N)$, we denote by $f \mapsto f_n$ the canonical map $\mathcal{G}_K^a(N) \rightarrow \mathcal{G}_K^a(n)$ induced by the projection $R_N \twoheadrightarrow R_n$. If v is a valuation of K we denote by $I_v(n) = \text{Hom}(K^\times / \mathcal{O}_v^\times, R_n) \leq \mathcal{G}_K^a(n)$ and $D_n(n) = \text{Hom}(K^\times / \pm (1 + \mathfrak{m}_v), R_n) \leq \mathcal{G}_K^a(n)$. For a subgroup $A \leq \mathcal{G}_K^a(n)$, we denote by A^\perp the subgroup of K^\times :

$$A^\perp = \bigcap_{f \in A} \ker f.$$

This is the left kernel of the canonical pairing $K^\times \times A \rightarrow R_n$.

The following notion of C-pairs is motivated by Bogomolov and Tschinkel's notion under the same name [BT02]; we note, however, that our notion of C-pairs is *a priori* much weaker than that considered in loc.cit..

Definition 2.1. Let $f, g \in \mathcal{G}_K^a(n)$ be given. We say that f, g are a C-pair provided that for all $x \in K \setminus \{0, 1\}$ one has:

$$f(1-x)g(x) = f(x)g(1-x).$$

A subgroup $A \leq \mathcal{G}_K^a(n)$ will be called a C-group provided that any pair of elements $f, g \in A$ form a C-pair. If $A = \langle f_i \rangle_i$, we observe that A is a C-group if and only if f_i, f_j form a C-pair for all i, j .

For a subgroup $A \leq \mathcal{G}_K^a(n)$, we denote by $\mathbf{I}^C(A)$ the subgroup:

$$\mathbf{I}^C(A) = \{f \in A : \forall g \in A, f, g \text{ form a C-pair}\}.$$

and call $\mathbf{I}^C(A)$ the C-center of A . In particular, A is a C-group if and only if $A = \mathbf{I}^C(A)$.

Theorem 3. Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(n)$. Let K be an arbitrary field and let $f, g \in \mathcal{G}_K^a(n)$ be given. Assume that there exist $f'', g'' \in \mathcal{G}_K^a(N)$ such that

- f'', g'' form a C-pair.
- $f''_n = f$ and $g''_n = g$.

Then there exists a valuation v of K such that

- $f, g \in D_v(n)$
- $\langle f, g \rangle / \langle f, g \rangle \cap I_v(n)$ is cyclic (possibly trivial).

Proof. The proof of this theorem is highly technical and involves a lot of calculation. For the sake of exposition, we defer the proof to §A. \square

3. COMPARABILITY OF VALUATIONS

In this section we prove the main theorems which allow us to detect valuations using C-pairs in a more precise way. To begin, we introduce the notion of a valutive subgroup $I \leq \mathcal{G}_K^a(n)$ which generalizes the notion of a “flag function” from [BT02]. For a valutive subgroup $I \leq \mathcal{G}_K^a(n)$ we associate a canonical valuation v_I which is reminiscent of Pop’s notion of a core of a valuation in a Galois extension, and was also considered in [AEJ87]. It turns out that the C-pair property is intimately related to the comparability of these canonical valuations v_I ; we will show that, in certain cases, we can “glue” valutive subgroups together.

In this section we will use results from the theory of rigid elements. While one can use many references in the subject to deduce these results (see e.g. the overview in the introduction), we will take [AEJ87] to be our reference of choice. We begin by recalling some minimal conditions for the existence of a valuation relative to a subgroup $H \leq K^\times$.

Lemma 3.1. Let K be a field and let $H \leq K^\times$ be given. The following are equivalent:

- (1) There exists a valuation v of K such that $\mathcal{O}_v^\times \leq H$.
- (2) $-1 \in H$, for all $x \in K^\times \setminus H$ one has $1+x \in H \cup xH$, and whenever $x, y \in K^\times \setminus H$ are such that $1+x, 1+y \in H$, one has $1+x(1+y) \in H$.

Proof. First assume that there exists a valuation v such that $\mathcal{O}_v^\times \leq H$. Let $x \in K^\times \setminus H$ be given. Then, in particular, $v(x) \neq 0$ and thus $1+x \in \mathcal{O}_v^\times$ iff $v(x) > 0$; also, $1+x \in x \cdot \mathcal{O}_v^\times$ iff $v(x) < 0$. Thus $1+x \in H \cup x \cdot H$ for all such x . Moreover, if $x, y \notin H$ and $1+x, 1+y \in H$ one has $v(x), v(y) > 0$ and thus $v(x \cdot (1+y)) > 0$ so that $1+x(1+y) \in H$ as required.

The converse is [AEJ87] Theorem 2.10 taking $T = H$ in loc.cit.. Indeed, observe that $1+x \in H \cup xH$ for all $x \in K^\times \setminus H$ iff $H + xH \subset H \cup xH$ for all $x \in K^\times \setminus H$ and that assumption (2) ensures the “preadditive” condition of loc.cit.. \square

Remark 3.2. In the case where $K^{\times \ell^n} \leq H$ and ℓ is odd, the condition of Lemma 3.1 can be made simpler. Using the notation of Lemma 3.1, the following are equivalent in this case:

- (1) There exists a valuation v of K such that $\mathcal{O}_v^\times \leq H$.
- (2) For all $x \in K^\times \setminus H$ one has $1+x \in H \cup xH$.

Again, see [AEJ87] Theorem 2.10 for the proof of the non-trivial direction of this claim.

Definition 3.3. A subgroup $H \leq K^\times$ will be called **valutive** if it satisfies the equivalent conditions of Lemma 3.1. Similarly, $I \leq \mathcal{G}_K^a(n)$ will be called valutive provided that I^\perp is valutive – equivalently there exists a valuation v of K such that $I \leq I_v(n)$. We also say

that $f \in \mathcal{G}_K^a(n)$ is valutive provided that $\ker(f)$ is valutive – equivalently there exists a valuation v of K such that $f \in I_v(n)$.

Lemma 3.4. *Let K be a field and let H be a valutive subgroup of K^\times . Then there exists a unique coarsest valuation v_H such that $\mathcal{O}_{v_H}^\times \leq H$. If w is a valuation of K such that $\mathcal{O}_w^\times \leq H$, then v_H is a coarsening of w ; moreover $w = v_H$ if and only if $w(H)$ contains no non-trivial convex subgroups.*

In particular, let $I \leq \mathcal{G}_K^a(n)$ be a valutive subgroup. Then there exists a unique coarsest valuation v_I , depending only on I , such that $I \leq I_{v_I}(n)$. If $I \leq I_w(n)$ then v_I is coarser than w . Moreover, $v_I = w$ if and only if $w(I^\perp)$ contains no non-trivial convex subgroups.

Proof. Let w be any valuation such that $\mathcal{O}_w^\times \leq H$ and consider the coarsening v of w which corresponds to the quotient of Γ_w by the maximal convex subgroup of $w(H)$. This is the coarsest coarsening v of w such that $\mathcal{O}_v^\times \leq H$. By construction, $v(H)$ contains no non-trivial convex subgroups. We deduce that whenever $x, y \in K^\times$ such that $v(x) = v(y) \pmod{v(H)}$ but $v(x) < v(y)$, there exists a $z \in K^\times$ such that $v(x), v(y) \neq v(z) \pmod{v(H)}$ and $v(x) < v(z) < v(y)$.

Now suppose $h \in H$ and $x \notin H$. Then $v(h) \neq v(x)$; moreover $v(h) < v(x)$ iff $h + x \in H$ and $v(h) > v(x)$ iff $h + x \in x \cdot H$. An element $h \in H$ such that $1 + x = h + x \pmod{H}$ for all $x \in K^\times \setminus H$ must be in \mathcal{O}_v^\times by the discussion above. We deduce that \mathcal{O}_v^\times depends only on H and K , but not at all on the original choice of w . Indeed, \mathcal{O}_v^\times is precisely the set of all $h \in H$ such that for all $x \in K^\times \setminus H$ one has $1 + x = h + x \pmod{H}$. \square

Definition 3.5. Suppose $H \leq K^\times$ is a valutive subgroup. We denote by v_H the canonical valuation associated to H as described in Lemma 3.4. I.e. v_H is the unique coarsest valuation such that $\mathcal{O}_{v_H}^\times \leq H$.

Similarly, suppose $I \leq \mathcal{G}_K^a(n)$ is valutive. We denote by v_I the valuation v_H for $H = I^\perp$. I.e. v_I is the unique coarsest valuation such that $I \leq I_{v_I}(n)$. If $f \in \mathcal{G}_K^a(n)$ is a given valutive element, we denote by $v_f := v_{\langle f \rangle} = v_{\ker f}$.

Lemma 3.6. *Let v_1, v_2 be two valuations and assume that f is a non-valuation element of $\mathcal{G}_K^a(n)$ such that $f \in D_{v_1}(n) \cap D_{v_2}(n)$. Then v_1, v_2 are comparable.*

Proof. Denote by w the valuation associated to the finest common coarsening of v_1, v_2 – i.e. $\mathcal{O}_w = \mathcal{O}_{v_1} \cdot \mathcal{O}_{v_2}$. Denote by $H = \ker f$. As $1 + \mathfrak{m}_{v_1}, 1 + \mathfrak{m}_{v_2} \leq H$, $H \neq K^\times$ and w is a coarsening of v_1, v_2 we deduce from the Approximation Theorem that w is non-trivial – indeed otherwise v_1, v_2 would be independent valuations and therefore $(1 + \mathfrak{m}_{v_1}) \cdot (1 + \mathfrak{m}_{v_2}) = K^\times$.

Consider $H_w \leq k(w)^\times$ the kernel of the canonical surjection $k(w)^\times \rightarrow \mathcal{O}_w^\times \cdot H/H$. Denote by $w_i = v_i/w$. One has $1 + \mathfrak{m}_{w_i} \leq H_w$ while, if both w_i are non-trivial, they must be independent. However, we note that $H_w \neq k(w)^\times$ since $\mathcal{O}_w^\times \cdot H/H \cong k(w)^\times/H_w$ and \mathcal{O}_w^\times is not contained in H by our assumption on f . In particular, either w_1 or w_2 must be trivial and so v_1, v_2 are comparable. \square

Proposition 3.7. *Let $f, g \in \mathcal{G}_K^a(n)$ be given valutive elements. Denote by $\Psi = (f, g)$. Then the following are equivalent:*

- (1) v_f and v_g are comparable.
- (2) $\langle f, g \rangle$ is valutive.
- (3) $\langle \Psi(1 - x), \Psi(x) \rangle$ is cyclic for all $x \in K^\times \setminus \{0, 1\}$.

Proof. Clearly (1) and (2) are equivalent by Lemma 3.4 and (2) \Rightarrow (3) is trivial (see e.g. Lemma 3.1 or the proof of Lemma 3.11). Thus, it remains to show that (3) \Rightarrow (2). Denote by $\Psi = (f, g)$ and denote by $T = \ker \Psi$. Assume that whenever $x \neq 0, 1$ one has:

$$\langle \Psi(1-x), \Psi(x) \rangle \text{ is cyclic.}$$

Since $\Psi(-1) = 0$, one equivalently has: $\langle \Psi(1+x), \Psi(x) \rangle$ is cyclic whenever $x \neq 0, -1$. Since R_n is a quotient of a discrete valuation ring, we deduce that this condition is equivalent to: $\Psi(1+x) = a \cdot \Psi(x)$ or $\Psi(x) = a \cdot \Psi(1+x)$ for some $a \in R_n$.

Let $x \notin T$ be given. As f, g are valutive, we recall that, for all $x \neq 0$ such that $f(x) \neq 0$, one has $f(1+x) = f(1)$ or $f(x)$ and similarly with g . Assume first that $\Psi(1+x) = a \cdot \Psi(x)$. Thus: $f(1+x) = af(x)$ and $g(1+x) = ag(x)$. We have some cases to consider. First, if $g(x) = 0$ or $f(x) = 0$ we trivially have $\Psi(1+x) = \Psi(1)$ or $\Psi(x)$. On the other hand, suppose $f(x), g(x) \neq 0$. Assume, for example, that $f(1+x) = f(x)$ and $g(1+x) = g(1) = 0$. Then $f(x) = af(x)$ and $ag(x) = 0$. But then a must be a unit in R_n (in fact $a \in 1 + \ell R_n$) and so $g(x) = 0$ – contradicting our assumption. We therefore deduce that $f(1+x) = f(x)$ iff $g(1+x) = g(x)$ and $f(1+x) = 0$ iff $g(1+x) = 0$. In particular, $\Psi(1+x) = \Psi(x)$ or $\Psi(1+x) = \Psi(1)$.

On the other hand, if $\Psi(x) = a\Psi(1+x)$ but $\ell|a$, this contradicts the fact that f and g are valutive and $\Psi(x) \neq 0$. Thus, we've shown that whenever $\Psi(x) \neq 0$ one has $\Psi(1+x) = \Psi(1)$ or $\Psi(1+x) = \Psi(x)$.

Assume now that $x, y \notin T$ are given such that $\Psi(1+x) = \Psi(1+y) = 0$. We will show that $\Psi(1+x(1+y)) = 0$. Observe that $\Psi(1+x(1+y)) = a\Psi(x)$ with $a = 0$ or $a = 1$, since $\Psi(1+y) = 0$ and $\Psi(x) = \Psi(x(1+y)) \neq 0$. Assume first that $\Psi(y) = -\Psi(x)$ then $f(x) = 0$ iff $f(y) = 0$ and $g(x) = 0$ iff $g(y) = 0$. If $f(x) = 0$ then $f(1+x(1+y)) = 0$ as well from the above and similarly for g . If $f(x) \neq 0$ then $f(1+x(1+y)) = 0$ since f is valutive and similarly for g .

On the other hand, assume that $\Psi(x) \neq -\Psi(y)$. Then $\Psi(1+x(1+y)) = \Psi(t+xy) = b\Psi(xy)$ for some $t \in T$ and $b = 0$ or $b = 1$. Furthermore, $\Psi(1+x(1+y)) = a \cdot \Psi(x)$ where $a = 0$ or $a = 1$, as above. But then $a\Psi(x) = b\Psi(xy)$, $a, b \in \{0, 1\}$, $\Psi(x), \Psi(y) \neq 0$ and $\Psi(xy) \neq 0$ – the only possibility for this is if $a, b = 0$. Now using Lemma 3.1, we deduce that T is indeed valutive – i.e. $\langle f, g \rangle$ is a valutive subgroup of $\mathcal{G}_K^a(n)$. \square

Remark 3.8. In this remark we will compare the condition of Proposition 3.7 with the C-pair property. Let $f, g \in \mathcal{G}_K^a(n)$ be given and denote by $\Psi = (f, g)$. Assume that $n = 1$ or $n = \infty$. Since R_n is a domain in this case, the following are equivalent:

- (1) $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic for all $x \neq 0, 1$.
- (2) f, g form a C-pair.

For general $n \in \overline{\mathbb{N}}$, however, this is completely false. However, we can say the following in general using our cancelation principle.

Let $n \in \overline{\mathbb{N}}$ be arbitrary and denote by $M = \mathbf{M}_1(n) = 2n - 1$ ($M = \mathbf{M}_1(\infty) = \infty$). Let $f, g \in \mathcal{G}_K^a(n)$ be given, denote by $\Psi = (f, g)$ and assume that $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic for all $x \neq 0, 1$. Then f, g trivially form a C-pair.

Conversely, assume that $f', g' \in \mathcal{G}_K^a(M)$ form a C-pair and denote by $\Psi = (f', g')$. Then $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic for all $x \neq 0, 1$. Indeed, assume, for example, that $g'(1-x) = ag'(x)$ (the other option is $g'(1-x) = bg'(x)$ and we simply replace x with $1-x$ in this case). As

$f'(1-x)g'(x) = f'(x)g'(1-x)$ we deduce that:

$$f'(1-x)g'(x) = f'(x)ag'(x).$$

By the cancelation principle, we deduce that, if $g(x) \neq 0$, one has $f(1-x) = af(x)$. Thus $\Psi(1-x) = a\Psi(x)$. On the other hand, $g(x) = 0$ implies that $g(1-x) = ag(x) = 0$ so that still $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic.

Using the fact that for any valuation v of K the canonical map $I_v(\mathbf{M}_1(n)) \rightarrow I_v(n)$ is surjective (since $\Gamma_v = K^\times / \mathcal{O}_v^\times$ is torsion-free), along with Proposition 3.7 and the discussion of Remark 3.8, we deduce the following fact which summarizes the discussion:

Lemma 3.9. *Let $f, g \in \mathcal{G}_K^a(n)$ be valutive elements. Then the following are equivalent:*

- (1) v_f and v_g are comparable.
- (2) $\langle f, g \rangle$ is valutive.
- (3) There exists a C-pair $f', g' \in \mathcal{G}_K^a(\mathbf{M}_1(n))$ such that $f'_n = f$, $g'_n = g$.

The results above allow us to say when a subgroup generated by valutive elements is itself valutive. Indeed, assume that I is valutive and $f \in I$; then v_f is a coarsening of v_I by Lemma 3.4. Thus, if $f_i \in \mathcal{G}_K^a(n)$ are valutive, then the following are equivalent:

- (1) $I = \langle f_i \rangle_i$ is valutive.
- (2) $v_i := v_{f_i}$ are comparable.

Moreover, when these equivalent statements hold, then v_I is the valuation-theoretic supremum of the v_i ; here we say that $w \leq v$ provided that w is a coarsening of v .

Lemma 3.10. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $M = \mathbf{M}_1(n)$. Let K be a field and let $f \in \mathcal{G}_K^a(M)$ be a valutive element. Suppose that $g \in \mathcal{G}_K^a(M)$ forms a C-pair with f . Denote by $v = v_{f_n}$. Then $g_n \in D_v(n)$.*

Proof. For sake of notation, we will assume that $n \in \mathbb{N}$, but the proof in the $n = \infty$ case is virtually identical. Let $x \in K^\times$ be given such that $v(x) > 0$ and $f(x) \neq 0 \pmod{\ell^n}$. Then $f(1-x) = 0 \pmod{\ell^n}$ implies that $f(1-x) = 0$ as well – indeed, f is valutive so $f(1-x) = f(1)$ or $f(x)$ and $f(x) \neq 0 \pmod{\ell^n}$. Then $f(1-x) = 0$ and thus $f(x)g(1-x) = 0$. Since $f(x) \neq 0 \pmod{\ell^n}$, we deduce from the cancelation principle that $g(1-x) = 0 \pmod{\ell^n}$.

On the other hand, if $v(y) > 0$ yet $f(y) = 0 \pmod{\ell^n}$, by Lemma 3.4, there exists x such that $0 < v(x) < v(y)$ and $f(x) \neq 0 \pmod{\ell^n}$. Now, by the first case, we deduce that $g(1-x) = 0 \pmod{\ell^n}$. Moreover, $v(x + y(1-x)) = v(x)$ and so $f(x + y(1-x)) = f(x) \neq 0 \pmod{\ell^n}$; thus $g((1-x)(1-y)) = g(1 - (x + y(1-x))) = 0 \pmod{\ell^n}$ by the first case. But this implies that $g(1-y) = 0 \pmod{\ell^n}$ as well. Therefore, $g(1 + \mathfrak{m}_v) = 0 \pmod{\ell^n}$, as required. \square

We are now ready to state the main theorem of the paper which deals with C-groups. This theorem, along with Theorem 11 gives a direct generalization of the analogous result from [Top12], and thus also the main theorem of [BT02].

Theorem 4. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_1(n))$. Let $D'' \leq \mathcal{G}_K^a(N)$ be given and assume that D'' is a C-group. Then $D := D''_n$ contains a valutive subgroup $I \leq D$ such that*

- D/I is cyclic.
- $D \leq D_{v_I}(n)$.

Proof. Denote by $M = \mathbf{M}_1(n)$ and $D' = D''_M$. Consider the subgroup I' of D' generated by all valutive elements $f \in D'$. By Theorem 3, D'/I' is cyclic. Moreover, by Lemma 3.9 and Remark 3.8, I' is valutive, since v_f and v_g are comparable for any $f, g \in I'$ as $\mathbf{N}(M) \geq \mathbf{M}_1(M)$; thus $I := I'_n$ is valutive as well. Moreover, by Lemma 3.10, for all $d \in D := D'_n$ and $i \in I$, one has $d \in D_{v_i}(n)$ and thus $D \leq D_{v_I}(n)$, as required. \square

Lemma 3.11. *Let $n \in \overline{\mathbb{N}}$ be given and let (K, v) be a valued field. Suppose that $d \in D_v(n)$ and $i \in I_v(n)$ and denote by $\Psi = (i, d)$. Then for all $x \in K^\times \setminus \{0, 1\}$ one has:*

$$\langle \Psi(1 - x), \Psi(x) \rangle \text{ is cyclic.}$$

In particular, i, d form a C-pair.

Proof. Denote by $\Psi = (i, d)$. If $x \in \mathcal{O}_v^\times$ then $i(x) = 0$ so the claim is trivial. On the other hand, if $v(x) > 0$ then $\Psi(1 - x) = 0$ since $1 + \mathfrak{m}_v \leq \ker \Psi$ so we obtain the claim. Lastly, if $v(x) < 0$ then $1 - x = x(1/x - 1)$ so that $\Psi(1 - x) = \Psi(x)$, and this completes the proof. \square

We now prove a theorem which allows us to detect the groups $I_v(n)$ within $D_v(n)$ in certain situations. This will be needed later on in order to detect precisely $I_v(n)$ and $D_v(n)$.

Theorem 5. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let $I'' \leq D'' \leq \mathcal{G}_K^a(N)$ be given and denote by $I = I''_n$ and $D = D''_n$. Assume that whenever $i \in I''$ and $d \in D''$, i, d form a C-pair (i.e. $I'' \leq \mathbf{I}^C(D'')$). Assume moreover that D is not a C-group. Then I is valutive and $D \leq D_{v_I}(n)$.*

Proof. Denote by $M = \mathbf{M}_1(n)$ and denote by $I' = I''_M$ and $D' = D''_M$. Since D is not a C-group and $D = D''_n$, we deduce that D' is not a C-group. Arguing as in Theorem 4, it suffices to prove that every $f \in I'$ is valutive. Assume for a contradiction that $f \in I'$ is non-valutive and let $g_1, g_2 \in D'$ be given such that $\langle f, g_i \rangle$ is non-cyclic – we will show that $\langle f, g_1, g_2 \rangle$ must form a C-group. Then, as we vary over all g_1, g_2 , we deduce that D' is a C-group as well which provides the required contradiction.

For the remainder of the proof, denote by $M' = \mathbf{M}_2(M) = \mathbf{M}_2(\mathbf{M}_1(n))$. Take lifts $f' \in I''_{M'}$ and $g'_i \in D''_{M'}$ for f resp. g_i . Then by Theorem 3, there exist valuations v_i such that:

- $\langle f', g'_i \rangle \in D_{v_i}(M')$
- $\langle f', g'_i \rangle / \langle f', g'_i \rangle \cap I_{v_i}(M')$ is cyclic.

For $i = 1$ and $i = 2$, we deduce that there exists $a_i f' + b_i g'_i \in I_{v_i}(M')$ where at least one of a_i, b_i is a unit; indeed otherwise $\langle f', g'_i \rangle \cap I_{v_i}(M')$ is contained in $\langle \ell \cdot f', \ell \cdot g'_i \rangle = \ell \cdot \langle f', g'_i \rangle$ but $\langle f', g'_i \rangle / \ell$ is non-cyclic by assumption.

Since f is non-valutive we deduce that $b_i g'_i \neq 0 \pmod{\ell^M}$. Indeed, if a_i is a unit and $b_i g'_i = 0 \pmod{\ell^M}$, this would imply that f is valutive; on the other hand, if b_i is a unit, then $b_i g'_i \neq 0 \pmod{\ell^M}$ since $g_i \neq 0 \pmod{\ell^M}$. Furthermore, since f' is non-valutive, the v_i must be comparable by Lemma 3.6. In particular, $\langle f', a_1 f' + b_1 g'_1, a_2 f' + b_2 g'_2 \rangle = \langle f', b_1 g'_1, b_2 g'_2 \rangle$ forms a C-group by Lemma 3.11 and Proposition 3.7. By the cancelation principle, $\langle f, g_1, g_2 \rangle$ form a C-group as well. Indeed, for all $x \in K^\times \setminus \{0, 1\}$ one has:

$$b_1 b_2 g'_1 (1 - x) g'_2(x) = b_1 b_2 g'_1(x) g'_2(1 - x)$$

and thus we also have $g_1(1 - x)g_2(x) = g_1(x)g_2(1 - x)$ since $b_1, b_2 \neq 0 \pmod{\ell^M}$ and $M' = \mathbf{M}_2(M)$. \square

4. DETECTING $D_v(n)$ AND $I_v(n)$

In this section, we show how to detect precisely the subgroups $D_v(n)$ and $I_v(n)$ for certain “maximal” valuations v . We also show that, in the case of function fields, these “maximal” valuations include the Parshin chains of divisors.

Let (K, v) be a valued field and $f \in D_v(n)$. Then the restriction $f|_{\mathcal{O}_v^\times}$ defines a homomorphism $f_v : k(v)^\times \rightarrow R_n$ such that $f_v(-1) = 0$. In particular this provides a canonical map $D_v(n) \rightarrow \mathcal{G}_{k(v)}^a(n)$. This map, in some sense, forces the C-pair property as we see in the following lemma; this lemma is an alternative stronger manifestation of Lemma 3.11.

Lemma 4.1. *Let (K, v) be a valued field and let $n \in \overline{\mathbb{N}}$ be given. The map $D_v(n) \rightarrow \mathcal{G}_{k(v)}^a(n)$ defined by $f \mapsto f_v$ induces an isomorphism $D_v(n)/I_v(n) \cong \mathcal{G}_{k(v)}^a(n)$. Let $f, g \in D_v(n)$ be given, then f, g form a C-pair if and only if their images f_v, g_v in $\mathcal{G}_{k(v)}^a(n)$ form a C-pair.*

Proof. Assume with no loss that $n \in \mathbb{N}$ as the $n = \infty$ case follows in the limit. Consider the short exact sequence:

$$1 \rightarrow k(v)^\times / \pm 1 \rightarrow K^\times / \pm (1 + \mathfrak{m}_v) \rightarrow \Gamma_v \rightarrow 1.$$

Tensoring this with \mathbb{Z}/ℓ^n and noting that Γ_v is torsion-free, we obtain:

$$1 \rightarrow (k(v)^\times / \ell^n) / \pm 1 \rightarrow (K^\times / \ell^n) / \pm (1 + \mathfrak{m}_v) \rightarrow \Gamma_v / \ell^n \rightarrow 1.$$

Taking $\text{Hom}(\bullet, \mathbb{Z}/\ell^n)$ we deduce that the following short sequence is exact by Pontryagin Duality:

$$1 \rightarrow I_v(n) \rightarrow D_v(n) \rightarrow \mathcal{G}_{k(v)}^a(n) \rightarrow 1.$$

If f, g form a C-pair then clearly f_v, g_v are a C-pair. Conversely, assume that f_v, g_v are a C-pair. Let $x \in K \setminus \{0, 1\}$ be given. If $v(x) > 0$ then $1 - x \in 1 + \mathfrak{m}_v \leq \ker f \cap \ker g$. Thus, $f(1 - x)g(x) = 0 = f(x)g(1 - x)$. If $v(x) < 0$ then $x^{-1}(1 - x) = x^{-1} - 1 \in -(1 + \mathfrak{m}_v)$ so that $(1 - x) \in -x \cdot (1 + \mathfrak{m}_v)$. Thus, $f(1 - x)g(x) = f(-x)g(x) = f(x)g(x) = f(x)g(-x) = f(x)g(1 - x)$. If $v(x) = 0$ and $v(1 - x) > 0$ we're in one of the previous cases with $y = 1 - x$. The last case to consider is where $x, 1 - x \in \mathcal{O}_v^\times$. Here, we note that $f(z) = f_v(\bar{z})$ (and similarly with g) for all $z \in \mathcal{O}_v^\times$ where $\bar{z} = z + \mathfrak{m}_v$ denotes the image of z in $k(v)^\times$. Thus, as f_v, g_v form a C-pair, we see that $f(x)g(1 - x) = f(1 - x)g(x)$ when $x, 1 - x \in \mathcal{O}_v^\times$. \square

Definition 4.2. Let $n \in \overline{\mathbb{N}}$ be given and denote by $N := \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field. We denote by $\mathcal{D}_{K,n}$ the collection of subgroups $D \leq \mathcal{G}_K^a(n)$ endowed with $I \leq D$ such that the following hold:

- (1) There exist $D' \leq \mathcal{G}_K^a(N)$ such that $(\mathbf{I}^C(D'))_n = I$, $D'_n = D$.
- (2) $I \leq D \leq \mathcal{G}_K^a(n)$ are maximal with this property. Namely, if $D \leq E \leq \mathcal{G}_K^a(n)$ and $E' \leq \mathcal{G}_K^a(N)$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^C(E'))_n$, then $D = E$ and $I = (\mathbf{I}^C(E'))_n$.
- (3) $\mathbf{I}^C(D) \neq D$ (i.e. D is not a C-group).

We denote by $\mathcal{W}_{K,n}$ the collection of valuations v of K such that:

- (1) Γ_v contains no non-trivial ℓ -divisible convex subgroups.
- (2) v is maximal among all valuations w such that $D_v^n = D_w^n$ and Γ_w contains no non-trivial ℓ -divisible convex subgroups; i.e. for all refinements w of v such that $D_w^n = D_v^n$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I_w^n = I_v^n$.

We also denote by $\mathcal{V}_{K,n}$ the collection of valuations $v \in \mathcal{W}_{K,n}$ such that $\mathcal{G}_{k(v)}^a(n)$ is non-cyclic.

Let $v \in \mathcal{V}_{K,n}$ be given. We furthermore introduce the following subsets:

- (1) We denote by $\mathcal{D}_{v,n}$ the subset of $\mathcal{D}_{K,n}$ consisting of $I \leq D$ such that $I_v(n) \leq I \leq D \leq D_v(n)$.
- (2) We denote by $\mathcal{W}_{v,n}$ the subset of $\mathcal{W}_{K,n}$ consisting of valuations finer than v .
- (3) We denote by $\mathcal{V}_{v,n}$ the subset of $\mathcal{V}_{K,n}$ consisting of valuations finer than v .

Example 4.3. We will say that a field k is **strongly ℓ -closed** provided that for any finite extension $k'|k$ one has $(k')^\times = (k')^{\times \ell}$; for example, algebraically closed fields of any characteristic and perfect fields of characteristic ℓ are strongly ℓ -closed. Observe that, if v_0 is a valuation of a strongly ℓ -closed field k , then $k(v_0)$ is also strongly ℓ -closed. In this example, we will show that geometric Parshin chains (i.e. compositions of valuations of a function field associated to Weil prime divisors) are elements of $\mathcal{W}_{K,n}$, where K is a function field over a strongly ℓ -closed field k . In particular, the non-degenerate Parshin chains of non-maximal length will lie in $\mathcal{V}_{K,n}$ while the non-degenerate maximal length Parshin chains will lie in $\mathcal{W}_{K,n} \setminus \mathcal{V}_{K,n}$.

This will be done in two steps. First, we show that valuations associated to Weil prime divisors lie in $\mathcal{W}_{K,n}$ for function fields $K|k$ as above. Second, we will show that compositions of valuations from \mathcal{W}_n lie in \mathcal{W}_n – this will hold for arbitrary fields.

Prime Divisors: Let K be a function field over a subfield k which is strongly ℓ -closed. Let v be the valuation associated to a prime Weil divisor on some model X of $K|k$. Then $v \in \mathcal{W}_{K,n}$.

In fact, we will prove much more. Suppose K is a field in which the polynomial $X^{2\ell^n} - 1$ splits completely. Let v be a valuation of K such that Γ_v contains no non-trivial ℓ -divisible convex subgroups and that $k(v)$ is a function field over a strongly ℓ -closed field k . Then $v \in \mathcal{W}_{K,n}$.

First, assume that $k(v)|k$ has transcendence degree ≥ 1 . Assume that w is a refinement of v and that $D_w(n) = D_v(n)$. Then $I_v(n) \leq I_w(n) \leq D_w(n) = D_v(n)$. We must show that $I_v(n) = I_w(n)$. Denote by $F = k(v)$ and consider the valuation $w/v =: w'$ of F induced by w . Observe that $I_v(n) = I_w(n)$ if and only if $I_{w'}(n) = 1$ as a subgroup of $\mathcal{G}_F^a(n)$ since we have a canonical isomorphism $I_w(n)/I_v(n) \cong I_{w/v}(n)$. Thus, we can assume without loss of generality that $n = 1$ (see e.g. Lemma 4.4 and the proof of Lemma 4.8).

Now assume that $0 \neq f \in I_{w'}(1)$ and denote by $T = \ker f$. Then $F^\times/T = \langle x \bmod T \rangle \cong \mathbb{Z}/\ell$. Furthermore, for all $g \in \mathcal{G}_F^a(1)$, f, g form a C-pair by Lemma 3.11. In particular, for all $H \leq F^\times$, $F^{\times \ell} \leq H$, such that $F^\times/H \cong \mathbb{Z}/\ell$, the group $\text{Hom}(F^\times/H \cap T, \mathbb{Z}/\ell)$ is a C-group.

Now assume that x, y are \mathbb{Z}/ℓ independent in F^\times/ℓ . Then we can choose T_0 such that $F^{\times \ell} \leq T_0 \leq T \leq F^\times$ and $F^\times/T_0 = \langle x, y \rangle \cong \mathbb{Z}/\ell \times \mathbb{Z}/\ell$. Thus, $\text{Hom}(F^\times/T_0, \mathbb{Z}/\ell)$ is a C-group. By the K-theoretic criterion for C-pairs (see Proposition 6.1, the proof of which is self-contained) we deduce, in particular, that $\{x, y\}_{T_0} \neq 0$ as an element of $K_2^M(F)/T_0$ (see § 6 for a review of the definition of Milnor K-theory mod T_0). In particular, $\{x, y\} \neq 0$ as an element of $K_2^M(F)/\ell$.

We will show that this provides a contradiction. First, since $x \notin F^{\times \ell}$ and k is strongly ℓ -closed, we deduce that x is transcendental over k . Consider the subfield $L = \overline{k(x)} \cap F$ the relative algebraic closure of $k(x)$ (the rational function field) inside F . Consider the unique complete normal model C for $L|k$ together with the (possibly branched) cover $C \rightarrow \mathbb{P}_k^1$ induced by $k(x) \rightarrow L$. By the approximation theorem, there exists a prime divisor P of \mathbb{P}_k^1

and a function $y \in k(x)^\times$ such that P is unramified in the cover $C \rightarrow \mathbb{P}_k^1$, $P \neq 0, \infty$, and $v_P(y) = 1$ (here v_P denotes the valuation associated to P). Since P is unramified in C , for any prolongation P' of P to C , one also has $v_{P'}(y) = 1$. Moreover, as $P \neq 0, \infty$ and the divisor associated to x is precisely $0 - \infty$, we deduce that the images of x, y are independent in $\text{Div}(C)/\ell$. Thus, their images are also independent in L^\times/ℓ .

On the other hand we recall a theorem of Milnor stating that the following sequence is exact:

$$0 \rightarrow K_2^M(k) \rightarrow K_2^M(k(x)) \rightarrow \bigoplus_{P \in \mathbb{A}_k^1} K_1^M(k(P)) \rightarrow 0$$

where the last map is the sum of the tame symbols associated to v_P , as P ranges over the prime divisors of \mathbb{P}_k^1 with support in $\mathbb{A}_k^1 = \text{Spec } k[x]$. However, the extension $k(P)|k$ is finite and thus $k(P)^{\times \ell} = k(P)^\times$ since k is strongly ℓ -closed. Also, this implies that $K_2^M(k)/\ell = 0$. Thus, we deduce that $K_2^M(k(x))/\ell = 0$ and so $\{x, y\} = 0$ in $K_2^M(F)/\ell$. Moreover, since L is relatively algebraically closed in F and x, y are independent in L^\times/ℓ , they must also be independent in F^\times/ℓ . This provides the desired contradiction to the discussion above, as we've produced an element $y \in F^\times$ such that x, y are independent in F^\times/ℓ and $\{x, y\} = 0$.

On the other hand, if the transcendence degree of $k(v)|k$ is 0, we observe that $k(v)^\times$ is ℓ -divisible since k is strongly ℓ -closed, and so $v \in \mathcal{W}_{K,n} \setminus \mathcal{V}_{K,n}$ trivially.

Compositions of Valuations: Let us furthermore show that compositions of valuations in \mathcal{W}_n lie in \mathcal{W}_n . Indeed, suppose that $v \in \mathcal{W}_{K,n}$ is given and $w \in \mathcal{W}_{k(v),n}$. Denote by $w' = w \circ v$ the valuation of K induced by w . By considering the short exact sequence:

$$1 \rightarrow \Gamma_w \rightarrow \Gamma_{w'} \rightarrow \Gamma_v \rightarrow 1$$

we see immediately that $\Gamma_{w'}$ contains no non-trivial ℓ -divisible convex subgroups. Furthermore, suppose that w'' is a refinement of w' such that $D_{w'}(n) = D_{w''}(n)$. Observe that v is a coarsening of w' , and thus of w'' . Since $D_w(n) = D_{w''/v}(n)$ we see that $I_w(n) = I_{w''/v}(n)$ (this is condition (2) for $w \in \mathcal{W}_{k(v),n}$); hence $I_{w'}(n) = I_{w''}(n)$.

We will now show how to detect $I_v(n)$ and $D_v(n)$ precisely for the valuations $v \in \mathcal{V}_{K,n}$. First, we note that when $\mathcal{G}_K(n)$ is cyclic, one cannot expect to detect anything. Indeed, first consider $K = \mathbb{C}((t))$. Then $\mathcal{G}_K^a(n)$ is cyclic by Kummer theory, the whole $\mathcal{G}_K^a(n)$ is valuative and its corresponding valuation is the t -adic one. On the other hand, we can consider $K = \overline{\mathbb{F}}_p^{\mathbb{Z}_\ell}$ ($p \neq \ell$) where \mathbb{Z}_ℓ is the Sylow- ℓ -subgroup of $\text{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$. By Kummer theory, $\mathcal{G}_K^a(n)$ is again cyclic, but K has no non-trivial valuations. Because of this observation and the compatibility in taking residue fields (see Lemma 4.1), one cannot expect to detect $I_v(n)$ within $D_v(n)$ when $\mathcal{G}_{k(v)}^a(n)$ is cyclic.

In light of Theorem 5, in order to detect $I_v(n)$ and $D_v(n)$, we need to ensure that the canonical maps $I_v(N) \rightarrow I_v(n)$ and $D_v(N) \rightarrow D_v(n)$ are surjective. The first map is indeed always surjective as Γ_v is torsion-free; however, the map $D_v(N) \rightarrow D_v(n)$ may not be surjective. However, it is surjective in two important cases which we consider below. First, if K contains sufficiently many roots of unity (and thus the same is true for $k(v)$) this map is surjective; here we do not restrict to fields K whose characteristic is different from ℓ . Secondly, if $N = n$, this map is trivially surjective; denoting $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$ as in Theorem 5, we see that $N = n$ iff $n = 1$ or $n = \infty$.

4.1. Sufficiently Many Roots of Unity.

Lemma 4.4. *Let (K, v) be a valued field. Let $N, n \in \overline{\mathbb{N}}$ be given, $N \geq n$ and assume furthermore that the polynomial $X^{2^{\ell^N}} - 1$ splits completely in K (we make no assumptions on $\text{char } K$); if $N = \infty$ we take this to mean that $X^{2^{\ell^m}} - 1$ splits for all $m \in \mathbb{N}$.*

(1) *The following canonical maps are surjective:*

- $\mathcal{G}_K^a(N) \rightarrow \mathcal{G}_K^a(n)$.
- $I_v(N) \rightarrow I_v(n)$.
- $D_v(N) \rightarrow D_v(n)$.

(2) *The rank of $\mathcal{G}_K^a(N)$ (as a pro- ℓ -group) is the same as that of $\mathcal{G}_K^a(n)$.*

(3) *Let $w \geq v$ be valuations of K and consider the inclusion of subgroups of $\mathcal{G}_K^a(N)$:*

$$I_v(N) \leq I_w(N) \leq D_w(N) \leq D_v(N).$$

Then $I_v(N) = I_w(N)$ iff $I_v(n) = I_w(n)$ and $D_w(N) = D_v(N)$ iff $D_w(n) = D_v(n)$.

Proof. Proof of (1): This is trivial if $n = \infty$, and thus we can assume that both $N, n \in \mathbb{N}$ as the case where $N = \infty$ would follow immediately from this. The Pontryagin dual of the map $\mathcal{G}_K^a(N) \rightarrow \mathcal{G}_K^a(n)$ is precisely the map:

$$K^\times / \ell^n \xrightarrow{\ell^{N-n}} K^\times / \ell^N.$$

Indeed our assumption that $X^{2^{\ell^N}} - 1$ splits completely ensures that $-1 \in K^{\times \ell^N}$. Thus, it suffices to prove that this map is injective. Suppose $x \in K^\times$ is given such that $x^{\ell^{N-n}} = y^{\ell^N}$. Then $x = y^{\ell^n} \cdot \zeta$ for some ζ such that $\zeta^{\ell^{N-n}} = 1$. But our assumptions ensure that $\zeta \in K^{\times \ell^n}$ which shows that indeed this map is injective. Dually, the map $\mathcal{G}_K^a(N) \rightarrow \mathcal{G}_K^a(n)$ is surjective.

The second claim is trivial as $\Gamma_v = K^\times / \mathcal{O}_v^\times$ is torsion-free. The proof of the third claim follows from the first one applied to $k(v)$, along with the fact that $D_v(N)/I_v(N) = \mathcal{G}_{k(v)}^a(N)$ and $D_v(n)/I_v(n) = \mathcal{G}_{k(v)}^a(n)$. Indeed, the fact that $X^{2^{\ell^N}} - 1$ splits in K implies that the same polynomial splits in $k(v)$ so that the map $\mathcal{G}_{k(v)}^a(N) \rightarrow \mathcal{G}_{k(v)}^a(n)$ is surjective.

Proof of (2): As above, we can assume with no loss that $N, n \in \mathbb{N}$. Arguing as in part (1), one has:

$$\ell^n \cdot \mathcal{G}_K^a(N) = \text{Hom}(K^\times / \pm 1, \ell^n \cdot R_N).$$

Thus the surjective map $\mathcal{G}_K^a(N) \rightarrow \mathcal{G}_K^a(n)$ corresponds precisely to $\mathcal{G}_K^a(N) \rightarrow \mathcal{G}_K^a(N)/\ell^n = \mathcal{G}_K^a(n)$ and this proves the claim using the Burnside basis theorem.

Proof of (3): By (1), $I_v(N) = I_w(N)$ implies that $I_v(n) = I_w(n)$ and similarly $D_v(N) = D_w(N)$ implies that $D_v(n) = D_w(n)$. To prove the converse it suffices to assume that v is the trivial valuation by replacing K with $k(v)$ and w by w/v ; indeed $I_w(n)/I_v(n) = I_{w/v}(n)$ and $D_w(n)/I_v(n) = D_{w/v}(n)$ – see e.g. the first part of Lemma 4.1. As such, assume that $I_w(n) = 1$ then $\Gamma_w = \ell^n \cdot \Gamma_w$ and so $\Gamma_w = \ell^N \cdot \Gamma_w$ since Γ_w is torsion-free; this implies that $I_w(N) = 1$. On the other hand, assume that $D_w(n) = \mathcal{G}_K^a(n)$. Then $1 + \mathfrak{m}_w \leq K^{\times \ell^n}$. Let $x \in 1 + \mathfrak{m}_v$ be given then $x = y^{\ell^n}$ for some $y \in K^\times$. Applying w to both sides we deduce that $y \in \mathcal{O}_w^\times$. Denote by $a \mapsto \bar{a}$ the map $\mathcal{O}_w^\times \rightarrow k(w)^\times$. Then $\bar{y}^{\ell^n} = \bar{1}$ so that there exists a $\bar{z} \in k(w)^\times$ such that $\bar{z}^{\ell^{N-n}} = \bar{y}$; indeed, we recall that the polynomial $X^{\ell^N} - 1$ splits in K . Thus, $y = z^{\ell^{N-n}} \cdot a$ for some $a \in 1 + \mathfrak{m}_w$. And thus $x = z^{\ell^N} a^{\ell^n}$. But as $a \in K^{\times \ell^n}$ we deduce that $a^{\ell^n} \in K^{\times \ell^{2n}}$. Proceeding inductively, we deduce in this way that $x \in K^{\times \ell^N}$. This shows that, indeed $D_w(N) = \mathcal{G}_K^a(N)$, as required. \square

Proposition 4.5. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_1(n))$. Let K be a field and assume that $X^{2\ell^N} - 1$ splits completely in K (we do not make any assumptions on $\text{char } K$). Let $D \leq \mathcal{G}_K^a(n)$ be given. Then the following are equivalent:*

- (1) *There exists a valuation v of K such that $D \leq D_v(n)$ and $D/D \cap I_v(n)$ is cyclic.*
- (2) *There exists a subgroup $D' \leq \mathcal{G}_K^a(N)$ such that D' is a C-group and $D'_n = D$.*

Proof. First assume that D' exists as above. Then the claim follows from Theorem 4. Conversely, assume that there exists a valuation v of K such that $D \leq D_v(n)$ and $D/D \cap I_v(n)$ is cyclic. Denote by $I = D \cap I_v(n)$ and choose $f \in D$ such that $\langle I, f \rangle = D$. Choose $f' \in D_v(N)$ a lifting of f via Lemma 4.4 and consider the pre-image $I' \leq I_v(N)$ of $I \leq I_v(n)$ under the surjective map $I_v(N) \rightarrow I_v(n)$. Then $I'_n = I$ and $f'_n = f$. Moreover, by Lemma 3.11, we see that $\langle I', f' \rangle$ is a C-group, as required. \square

Proposition 4.6. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field and assume that $X^{2\ell^N} - 1$ splits completely in K (we do not make any assumptions on $\text{char } K$). Assume that $\mathbf{I}^C(\mathcal{G}_K^a(n)) \neq \mathcal{G}_K^a(n)$, consider $I' = \mathbf{I}^C(\mathcal{G}_K^a(N))$ and denote by $I = I'_n$. Then I is valutive, $v := v_I \in \mathcal{V}_{K,n}$, $I = I_v(n)$ and $D_v(n) = \mathcal{G}_K^a(n)$.*

Proof. We know that I is valutive and, denoting $v = v_I$, $D_v(n) = \mathcal{G}_K^a(n)$ from Theorem 5. On the other hand, $D_v(N) = \mathcal{G}_K^a(N)$ by Lemma 4.4 and so we see that $I_v(N) \leq I'$ by Lemma 3.11; thus $I_v(n) \leq I \leq I_v(n)$ so that $I = I_v(n)$.

Let us show that $v \in \mathcal{W}_{K,n}$. Suppose that w is a refinement of v such that $D_v(n) = \mathcal{G}_K^a(n) = D_w(n)$. Then, as above, $I_w(N) \leq I'$ so that $I_w(n) \leq I_v(n) \leq I_w(n)$ and thus $I_w(n) = I_v(n)$. Moreover, $\mathcal{G}_K^a(n)/I$ is non-cyclic since $\mathcal{G}_K^a(n)$ is not a C-group; thus we see that $v \in \mathcal{V}_{K,n}$. \square

Theorem 6. *Let $n \in \mathbb{N}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field and assume that $X^{2\ell^N} - 1$ splits completely in K (we do not make any assumptions on $\text{char } K$). Let $I \leq D \leq \mathcal{G}_K^a(n)$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v(n)$ and $D = D_v(n)$ if and only if the following holds:*

- (1) *There exist $D' \leq \mathcal{G}_K^a(N)$ such that $(\mathbf{I}^C(D'))_n = I$, $D'_n = D$.*
- (2) *$I \leq D \leq \mathcal{G}_K^a(n)$ are maximal with this property. Namely, if $D \leq E \leq \mathcal{G}_K^a(n)$ and $E' \leq \mathcal{G}_K^a(N)$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^C(E'))_n$, then $D = E$ and $I = (\mathbf{I}^C(E'))_n$.*
- (3) *$\mathbf{I}^C(D) \neq D$ (i.e. D is not a C-group).*

Proof. Let $I \leq D$ be given which satisfy conditions (1)-(3) as above. Then I is valutive and $D \leq D_v(n)$, where $v = v_I$, by Theorem 5. Consider $I' = I_v(N) \leq D_v(N) = D'$. By Lemma 4.4, one has $I'_n = I_v(n)$ and $D'_n = D_v(n)$. Furthermore, by Lemma 3.11, $I' \leq \mathbf{I}^C(D')$. Thus, $I \leq I_v(n) = I'_n \leq (\mathbf{I}^C(D'))_n =: J$ and $D \leq D_v(n) = D'_n$. By assumption (2) on $I \leq D$ we deduce that $I = J$ and $D = D_v(n)$. Moreover, by Theorem 5, J is valutive and $D_v(n) \leq D_{v_J}(n)$. But $I_v(n) \leq J \leq I_{v_J}(n)$ implies that v is coarser than v_J so that $D_{v_J}(n) \leq D_v(n)$. Thus, $D_v(n) = D_{v_J}(n)$ and $I = I_v(n)$, as required.

Since $v = v_I$, we see immediately by the definition of v_I that Γ_v contains no non-trivial convex ℓ -divisible subgroups so that v satisfies assumption (1) of $\mathcal{W}_{K,n}$. Assume that w is a refinement of v (i.e. v is coarser than w) such that $D_v(n) = D_w(n)$. Then $I_v(n) \leq I_w(n) \leq D_w(n) = D_v(n)$. But then:

$$I_v(n) \leq I_w(n) \leq (\mathbf{I}^C(D_w(N)))_n \leq (D_w(N))_n = D_w(n) = D_v(n)$$

implies that $I_v(n) = I_w(n)$ by assumption (2) on $I \leq D$ – thus $v \in \mathcal{W}_{K,n}$. Moreover, $\mathcal{G}_{k(v)}^a(n) = D_v(n)/I_v(n)$ is non-cyclic as $D_v(n)$ is not a C-group by assumption (3) (see Lemma 3.11), so we deduce that $v \in \mathcal{V}_{K,n}$.

Conversely assume that $v \in \mathcal{V}_{K,n}$ is given. By Lemma 3.11, we have $I_v(N) \leq \mathbf{I}^C(D_v(N)) \leq D_v(N)$ and by Lemma 4.4 we obtain:

$$I_v(n) \leq (\mathbf{I}^C(D_v(N)))_n \leq D_v(n).$$

Moreover, $I := (\mathbf{I}^C(D_v(N)))_n$ is valutive and $D_v(n) \leq D_{v_I}(n)$ by Theorem 5. Since $I_v(n) \leq I$, v_I is a refinement of v and so $D_v(n) = D_{v_I}(n)$ since then $D_{v_I}(n) \leq D_v(n) \leq D_{v_I}(n)$. Thus, $I_v(n) = I$ by our assumption (2) on v .

Let us now show that $I := I_v(n) \leq D_v(n) =: D$ satisfy the condition (2) required by $\mathcal{D}_{K,n}$. Assume that $E' \leq \mathcal{G}_K^a(N)$ and $D \leq E := E'_n$ and $I \leq (\mathbf{I}^C(E'))_n =: J$. By Theorem 5, J is valutive and $D \leq E \leq D_w(n)$ where $w = v_J$. But since $I \leq J \leq D_w(n)$, v is a coarsening of w and so, similarly to above, we deduce that $D = D_w(n)$. Now the condition (2) of v ensures that $I_v(n) = I_w(n) = I$, as required.

Lastly, we must show that D is not a C-group – i.e. condition (3) of $I \leq D$. Assume for a contradiction that D is a C-group; equivalently, $\mathcal{G}_{k(v)}^a(n)$ is a C-group by Lemma 4.1. However, $\mathcal{G}_{k(v)}^a(n)$ is non-cyclic and thus $\mathcal{G}_{k(v)}^a(1)$ is non-cyclic as well by Lemma 4.4. But $\mathcal{G}_{k(v)}^a(n)$ being a C-group implies that $\mathcal{G}_{k(v)}^a(1)$ is a C-group as well. Thus, applying Theorem 4 with $n = 1$, there exists a valutive subgroup $J \leq \mathcal{G}_{k(v)}^a(1)$ such that $\mathcal{G}_{k(v)}^a(1) = D_{w'}(1)$ where $w' = v_J$ and $D_{w'}(1)/I_{w'}(1)$ is cyclic. But by Lemma 4.4, $D_{w'}(n) = \mathcal{G}_{k(v)}^a(n)$ and $D_{w'}(n)/I_{w'}(n)$ is cyclic as well. Denote by $w = v \circ w'$ so that $I_v(n) \leq I_w(n) \leq D_w(n) = D_v(n)$, with $D_w(n)/I_w(n)$ cyclic. But this contradicts condition (2) of $v \in \mathcal{W}_{K,n}$ as $D_v(n)/I_v(n) = \mathcal{G}_{k(v)}^a(n)$ is non-cyclic (since $v \in \mathcal{V}_{K,n}$) and thus $I_v(n) \neq I_w(n)$. \square

Remark 4.7. Let $n \in \overline{\mathbb{N}}$ be given. Suppose that K is a field in which the polynomial $X^{2\ell^n} - 1$ splits completely for $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Then map $v \mapsto I_v(n) \leq D_v(n)$ defines a bijection $\mathcal{V}_{K,n} \rightarrow \mathcal{D}_{K,n}$.

Let $v \in \mathcal{V}_{K,n}$ be given. By Lemma 4.1, the bijection $\mathcal{V}_{K,n} \rightarrow \mathcal{D}_{K,n}$ restricts to a bijection $\mathcal{V}_{v,n} \rightarrow \mathcal{D}_{v,n}$. Furthermore, this restricted bijection is compatible with the bijection $\mathcal{V}_{k(v),n} \rightarrow \mathcal{D}_{k(v),n}$ via the canonical bijections $\mathcal{V}_{k(v),n} \rightarrow \mathcal{V}_{v,n}$ and $\mathcal{D}_{k(v),n} \rightarrow \mathcal{D}_{K,n}$.

We conclude this subsection by providing an alternative definition of $\mathcal{V}_{K,n}$, as promised in Remark 1.2 from the introduction.

Lemma 4.8. *Let $n \in \overline{\mathbb{N}}$ be given and let K be a field in which $X^{2\ell^n} - 1$ splits completely. Then $\mathcal{V}_{K,n}$ is precisely the collection of valuations v of K such that:*

- (1) Γ_v contains no non-trivial ℓ -divisible convex subgroups.
- (2) $I_v(1) = \mathbf{I}^C(D_v(1)) \neq D_v(1)$.

In particular, $\mathcal{V}_{K,n} = \mathcal{V}_{K,m}$ for all $m \leq n$.

Proof. The argument of this lemma is similar to that of Theorem 6. Denote by \mathcal{V} the collection of valuations satisfying the two conditions (1),(2) above. First, let us show that $\mathcal{V} \subset \mathcal{V}_{K,n}$. Let $v \in \mathcal{V}$ be given; we need show the following conditions:

- (a) Γ_v contains no non-trivial ℓ -divisible convex subgroups.
- (b) If w is a refinement of v such that $D_w(n) = D_v(n)$ then $I_w(n) = I_v(n)$.

(c) $\mathcal{G}_{k(v)}^a(n)$ is non-cyclic.

Condition (1) for $v \in \mathcal{V}$ is precisely (a). First, as $\mathbf{I}^C(D_v(1)) \neq D_v(1)$, we see that $\mathcal{G}_{k(v)}^a(n) = D_v(n)/I_v(n)$ is non-cyclic since $I_v(n) \leq \mathbf{I}^C(D_v(n))$. Suppose then w is a refinement of v such that $D_w(n) = D_v(n)$. Consider $I_v(1) \leq I_w(1) \leq D_w(1) \leq D_v(1)$. Moreover, by Lemma 3.11, we see that:

$$\mathbf{I}^C(D_v(1)) = I_v(1) \leq I_w(1) \leq \mathbf{I}^C(D_v(1)) \leq D_w(1) = D_v(1).$$

Thus, $I_w(1) = I_v(1)$, and by Lemma 4.4, we see that $I_w(n) = I_v(n)$ as well.

Conversely we show that $\mathcal{V}_{K,n} \subset \mathcal{V}$; assume that $v \in \mathcal{V}_{K,n}$. Then condition (1) of \mathcal{V} holds trivially. Let us show that $I_v(1) = \mathbf{I}^C(D_v(1)) \neq D_v(1)$. Clearly, $I_v(1) \leq \mathbf{I}^C(D_v(1))$ by Lemma 3.11. Denote by $I = \mathbf{I}^C(D_v(1))$. Then by Theorem 5, I is valutive and, denoting by $w = v_I$, one has $D_v(1) \leq D_w(1)$. Since w is a refinement of v we see that $D_w(1) = D_v(1)$ and thus $D_w(n) = D_v(n)$ by Lemma 4.4. By the definition of $\mathcal{V}_{K,n}$ we see that $I_w(n) = I_v(n)$ and thus $I \leq I_w(1) = I_v(1) \leq I$ so that $I = I_v(1)$. Also, $\mathcal{G}_{k(v)}^a(n)$ is non-cyclic and thus $\mathcal{G}_{K(v)}^a(1)$ is non-cyclic by Lemma 4.4 – in particular, $D_v(1)/I$ cannot be cyclic, as required. \square

4.2. The $n = 1$ or $n = \infty$ Case. Throughout this subsection, n will denote either 1 or ∞ . The key property to notice is that R_n is a domain and that $\mathbf{N}(n) = \mathbf{M}_r(n) = n$ (in fact, 1 and ∞ are the only fixed points of \mathbf{N} and of \mathbf{M}_r). The proofs of the results below are virtually identical (and in fact much easier) to those in §4.1 using this observation. Indeed, the added assumption that $X^{2\ell^N} - 1$ splits in K was only used in the fact that $D_v(N) \rightarrow D_v(n)$ is surjective. In this case, $N = n$ so that this is trivially satisfied. We therefore omit the proofs in this subsection.

Proposition 4.9. *Let $n = 1$ or $n = \infty$ and let K be an arbitrary field. Let $D \leq \mathcal{G}_K^a(n)$ be given. Then the following are equivalent:*

- (1) *There exists a valuation v of K such that $D \leq D_v(n)$ and $D/D \cap I_v(n)$ is cyclic.*
- (2) *D is a C -group.*

Proposition 4.10. *Let $n = 1$ or $n = \infty$ and let K be an arbitrary field. Assume that $\mathbf{I}^C(\mathcal{G}_K^a(n)) \neq \mathcal{G}_K^a(n)$ and consider $I = \mathbf{I}^C(\mathcal{G}_K^a(n))$. Then I is valutive, $v := v_I \in \mathcal{V}_{K,n}$, $I = I_v(n)$ and $D_v(n) = \mathcal{G}_K^a(n)$.*

Theorem 7. *Let $n = 1$ or $n = \infty$. Let K be an arbitrary field and let $I \leq D \leq \mathcal{G}_K^a(n)$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v(n)$ and $D = D_v(n)$ if and only if the following holds:*

- (1) $I = \mathbf{I}(D)$.
- (2) $I \leq D \leq \mathcal{G}_K^a(n)$ are maximal with this property. Namely, if $D \leq E \leq \mathcal{G}_K^a(n)$ and $I \leq \mathbf{I}^C(E)$, then $D = E$ and $I = \mathbf{I}^C(E)$.
- (3) $\mathbf{I}^C(D) \neq D$ (i.e. D is not a C -group).

Remark 4.11. Suppose that K is an arbitrary field and $n = 1$ or $n = \infty$. Then map $v \mapsto I_v(n) \leq D_v(n)$ defines a bijection $\mathcal{V}_{K,n} \rightarrow \mathcal{D}_{K,n}$.

Let $v \in \mathcal{V}_{K,n}$ be given. By Lemma 4.1, the bijection $\mathcal{V}_{K,n} \rightarrow \mathcal{D}_{K,n}$ restricts to a bijection $\mathcal{V}_{v,n} \rightarrow \mathcal{D}_{v,n}$. Furthermore, this restricted bijection is compatible with the bijection $\mathcal{V}_{k(v),n} \rightarrow \mathcal{D}_{k(v),n}$ via the canonical bijections $\mathcal{V}_{k(v),n} \rightarrow \mathcal{V}_{v,n}$ and $\mathcal{D}_{k(v),n} \rightarrow \mathcal{D}_{K,n}$.

5. RESTRICTING THE CHARACTERISTIC

In this section we provide conditions which distinguish which valuations have residue characteristic $\neq \ell$ for those valuations detected in Theorems 3, 4 and 5.

Throughout this section we fix $n \in \overline{\mathbb{N}}$. Let $L|K$ be an extension of fields. We will denote the restriction map $\mathcal{G}_L^a(n) \rightarrow \mathcal{G}_K^a(n)$ by $f \mapsto f_K$. For a subgroup $H \leq K^\times$ we denote by $L_H = K(\sqrt[n]{H})$ (if $n = \infty$ we denote $K(\sqrt[n]{H}) := \bigcup_{m \in \mathbb{N}} K(\sqrt[m]{H})$) and for a subgroup $A \leq \mathcal{G}_K^a(n)$ we denote by $L_A = L_{A^\perp}$.

Lemma 5.1. *Let $n \in \overline{\mathbb{N}}$ be given. Let (K, v) be a valued field such that $\text{char } K \neq \ell$. Denote by $L = K(\sqrt[n]{1 + \mathfrak{m}_v})$ and w a chosen prolongation of v to L . Let Δ be the convex subgroup of Γ_v generated by $v(\ell)$ (this is trivial unless $\text{char } k(v) = \ell$). Then $\Delta \leq \ell^n \cdot \Gamma_w$ (here we denote by $\ell^\infty \Gamma_v = \bigcap_{m \in \mathbb{N}} \ell^m \Gamma_v$).*

Proof. We can assume with no loss that $n \in \mathbb{N}$ as the $n = \infty$ case follows from this. If $\text{char } k(v) \neq \ell$ then $v(\ell) = 0$ and the lemma is trivial. So assume that $\text{char } k(v) = \ell$. Let $x \in K^\times$ be such that $0 < v(x) \leq v(\ell)$ and so $1 + x \in L^{\times \ell^n}$. Take $y \in L$ such that $1 + x = (1 + y)^{\ell^n}$. Note that $y \in \mathcal{O}_w$ and, since $1 + x = (1 + y)^{\ell^n} = 1 + y^{\ell^n} \pmod{\mathfrak{m}_w}$, we deduce that $y \in \mathfrak{m}_w$. Expanding the equation $1 + x = (1 + y)^{\ell^n}$ we see that $x = \ell \cdot y \cdot \epsilon + y^{\ell^n}$ for some $\epsilon \in \mathcal{O}_w$. But $w(x) \leq w(\ell) < w(\ell \cdot y \cdot \epsilon)$ since $w(y) > 0$ and $w(\epsilon) \geq 0$; thus, $w(x) = w(y^{\ell^n})$ by the ultrametric inequality. \square

Proposition 5.2. *Let $n \in \overline{\mathbb{N}}$ be given. Let K be a field such that $\text{char } K \neq \ell$. Suppose that $I \leq \mathcal{G}_K^a(n)$ and $D \leq \mathcal{G}_K^a(n)$ are given. Denote by $L = L_D$ and assume that there exists $I' \leq \mathcal{G}_L^a(n)$ such that I' is valutive (denote $w' = v_{I'}$ and $w = w'|_K$), $I'_K = I$ and $D \leq D_w(n)$. Then I is valutive, $D \leq D_{v_I}(n)$ and $\text{char } k(v_I) \neq \ell$.*

Proof. First, as I' is valutive and $I = I'_K$, we see that $I \leq I_w(n)$ and is indeed valutive. Moreover, as $D \leq D_w(n)$ and $v_I =: v$ is a coarsening of w , we see that $D \leq D_v(n)$ as well; indeed, recall that v is the coarsening of w which corresponds to the maximal convex subgroup of $w(I^\perp)$. On the other hand, since $D \leq D_w(n)$ we see that $\sqrt[n]{1 + \mathfrak{m}_w} \subset L$.

Denote by Δ the convex subgroup of Γ_w generated by $w(\ell)$. If $n \in \mathbb{N}$, we consider the canonical injective map induced by taking the dual of the surjective map $I' \twoheadrightarrow I$:

$$\Gamma_w/w(I^\perp) \hookrightarrow \Gamma_{w'}/w'((I')^\perp).$$

By Lemma 5.1, we deduce that $\Delta \leq w(I^\perp)$ since $\Delta \leq \ell^n \cdot \Gamma_{w'} \leq w'((I')^\perp)$. Therefore, Δ is contained in the kernel of the canonical projection $\Gamma_w \rightarrow \Gamma_v$. In particular, $v(\ell) = 0$ so that $\text{char } k(v) \neq \ell$.

On the other hand, if $n = \infty$, the \mathbb{Z}_ℓ -dual of $I' \twoheadrightarrow I$ is the injective map:

$$\widehat{\Gamma}_w/\widehat{w}(I^\perp) \hookrightarrow \widehat{\Gamma}_{w'}/\widehat{w}'((I')^\perp).$$

Observe that the image of Δ lies in the kernel of this map. Thus, the image of Δ under the map $\Gamma_w \rightarrow \widehat{\Gamma}_w$ is contained in $\widehat{w}(I^\perp)$; therefore, we still see that Δ is contained in the kernel of $\Gamma_w \twoheadrightarrow \Gamma_v$ since the kernel of $\Gamma_w \rightarrow \widehat{\Gamma}_w$ is $\ell^\infty \cdot \Gamma_w \leq w(I_w(\infty)^\perp)$. \square

We now prove three theorems which are analogous to the main results of §3; however, here we show how to ensure that the valuations produced have residue characteristic different from ℓ provided the same is true for K .

Theorem 8. Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(n)$. Let K be a field such that $\text{char } K \neq \ell$, let $f, g \in \mathcal{G}_K^a(n)$ be given and denote by $L = L_H$ where $H = \ker f \cap \ker g$. Assume that there exist $f'', g'' \in \mathcal{G}_L^a(N)$ such that

- f'', g'' form a C-pair.
- $(f'')_K = f$ and $(g'')_K = g$.

Then there exists a valuation v of K such that

- $f, g \in D_v(n)$
- $\langle f, g \rangle / \langle f, g \rangle \cap I_v(n)$ is cyclic (possibly trivial).
- $\text{char } k(v) \neq \ell$.

Proof. Denote by $f' = f''_n$ and $g' = g''_n$. Then by Theorem 3, there exists a valuation w' of L such that $f', g' \in D_{w'}(n)$ and $\langle f', g' \rangle / \langle f', g' \rangle \cap I_{w'}(n)$ is cyclic. Denote by $w = w'|_K$, $I = (\langle f', g' \rangle \cap I_{w'}(n))_K$ and $D = \langle f, g \rangle$, and observe that $D \leq D_w(n)$. Thus, the claim follows from Proposition 5.2. \square

Theorem 9. Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_1(n))$. Let K be a field such that $\text{char } K \neq \ell$. Let $D \leq \mathcal{G}_K^a(n)$ be given and assume that there exists $D'' \leq \mathcal{G}_{L_D}^a(N)$ such that D'' is a C-group and that $D = (D'')_K$. Then there exists a valutive subgroup $I \leq D$ such that:

- D/I is cyclic.
- $D \leq D_{v_I}(n)$.
- $\text{char } k(v_I) \neq \ell$.

Proof. Denote by $L = L_D$ and $D' = D''_n \leq \mathcal{G}_L^a(n)$. By Theorem 4, there exists a valutive subgroup $I' \leq D'$ such that $D' \leq D_{w'}(n)$ where $w' = v_{I'}$ is the valuation of L corresponding to I' , and D'/I' is cyclic. Denote by $I = I'_K$; then D/I is cyclic as $D = D'_K$; moreover, observe that $D \leq D_w(n)$ where $w = w'|_K$. By Proposition 5.2, I is valutive, $\text{char } k(v_I) \neq \ell$ and $D \leq D_{v_I}(n)$, as required. \square

Theorem 10. Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that $\text{char } K \neq \ell$. Let $I \leq D \leq \mathcal{G}_K^a(n)$ be given and denote by $L = L_D$. Assume that there exists $I'' \leq D'' \leq \mathcal{G}_L^a(N)$ such that $I'' \leq \mathbf{I}^C(D'')$, $(I'')_K = I$, $(D'')_K = D$, and that $D \neq \mathbf{I}^C(D)$. Then I is valutive, $D \leq D_{v_I}(n)$ and $\text{char } k(v_I) \neq \ell$.

Proof. The proof of this theorem is similar to the proof of Theorem 9 using Theorem 5 instead of Theorem 4 along with, again, Proposition 5.2. \square

Remark 5.3. Using Theorem 8 resp. 9 resp. 10 instead of Theorem 3 resp. 4 resp. 5, one can prove results analogous to those in §4 while considering only valuations whose residue characteristic is different from ℓ . We will not state these results explicitly, as their Galois-theoretical analogues are already stated in Theorem 2.

Part 2. Galois Theory and Milnor K-theory

6. MILNOR K-THEORY AND THE C-PROPERTY

Let K be any field. The usual construction of the Milnor K-ring is as follows:

$$K_n^M(K) = \frac{(K^\times)^{\otimes n}}{\langle a_1 \otimes \cdots \otimes a_n : \exists 1 \leq i < j \leq n, a_i + a_j = 1 \rangle}.$$

23

The tensor product makes $K_*^M(K) := \bigoplus_n K_n^M(K)$ into a graded-commutative ring and we denote by $\{\bullet, \bullet\}$ the product $K_1^M(K) \times K_1^M(K) \rightarrow K_2^M(K)$.

More generally, let $T \leq K^\times$ be given. We define $K_*^M(K)/T$ as the quotient of $K_*^M(K)$ by the graded ideal generated by $T \leq K^\times = K_1^M(K)$ or explicitly as follows:

$$K_n^M(K)/T = \frac{(K^\times/T)^{\otimes n}}{\langle a_1 \cdot T \otimes \cdots \otimes a_n \cdot T : \exists 1 \leq i < j \leq n, 1 \in a_i \cdot T + a_j \cdot T \rangle}.$$

Again, the tensor product makes $K_*^M(K)/T = \bigoplus_n K_n^M(K)/T$ into a graded-commutative ring and we denote the product in this ring by $\{\bullet, \bullet\}_T$. Moreover, one has a surjective map of graded-commutative rings: $K_*^M(K) \rightarrow K_*^M(K)/T$. It is well known that $\{x, -1\} = \{x, x\} \in K_2^M(K)$, for all $x \in K^\times$. Thus the same is true in $K_2^M(K)/T$; namely, $\{x, -1\}_T = \{x, x\}_T$. For more on the arithmetical properties of these canonical quotients of the Milnor K-ring, refer to Efrat [Efr06], [Efr07] where they are systematically studied.

In particular, suppose that $T \leq K^\times$ and $-1 \in T$. Then the canonical map $(K^\times/T) \otimes (K^\times/T) \rightarrow K_2^M(K)/T$ factors through

$$\wedge^2(K/T) = \frac{(K^\times/T) \otimes (K^\times/T)}{\langle x \otimes x : x \in K^\times/T \rangle}$$

Moreover, the kernel of the canonical surjective map $\wedge^2(K^\times/T) \rightarrow K_2^M(K)/T$ is generated by $z \wedge (1 - z)$ as z varies over the elements of $K^\times \setminus \{0, 1\}$.

Suppose that $n \in \mathbb{N}$, $\pm K^{\times \ell^n} \leq T \leq K^\times$ is given such that K^\times/T has rank 2. Say e.g. that:

$$K^\times/T = x^{\mathbb{Z}/\ell^{n-a}} \times y^{\mathbb{Z}/\ell^{n-b}} \cong \mathbb{Z}/\ell^{n-a} \times \mathbb{Z}/\ell^{n-b}.$$

Then $\wedge^2(K^\times/T)$ is generated by $x \wedge y$ and has order $\ell^{n-\max(a,b)}$. In particular, $K_2^M(K)/T = \langle \{x, y\}_T \rangle$ is cyclic of order ℓ^{n-c} where $c \geq \max(a, b)$. This observation will allow us to give a K-theoretic characterization of C-pairs.

Proposition 6.1 (K-theoretic characterization of C-pairs). *Let $n \in \mathbb{N}$ be given. Let $f, g \in \mathcal{G}_K^a(n)$ be given quasi-independent elements of order ℓ^{n-a} resp. ℓ^{n-b} ; in particular,*

$$\langle f, g \rangle = \langle f \rangle \oplus \langle g \rangle \cong (\mathbb{Z}/\ell^{n-a}) \cdot f \oplus (\mathbb{Z}/\ell^{n-b}) \cdot g.$$

Denote by $T = \ker f \cap \ker g$ and say that $K_2^M(K)/T$ has order ℓ^{n-c} . Then f, g form a C-pair if and only if $c \leq a + b$.

On the other hand, let $f, g \in \mathcal{G}_K^a(\infty)$ be given. Then f, g form a C-pair if and only if f_n, g_n form a C-pair for all $n \in \mathbb{N}$.

Proof. If $f, g \in \mathcal{G}_K^a(\infty)$, the fact that f, g form a C-pair if and only if f_n, g_n form a C-pair for all $n \in \mathbb{N}$ follows immediately from the definition. Let us therefore show the $n \in \mathbb{N}$ case, and note that a similar K-theoretic criterion for $n = \infty$ is given in Remark 6.3.

Let $n \in \mathbb{N}$ be given and let f, g be quasi-independent elements of $\mathcal{G}_K^a(n)$ as in the statement of the proposition. Thus, K^\times/T has quasi-independent generators which are dual to f, g which we denote by x, y :

$$K^\times/T = x^{\mathbb{Z}/\ell^{n-a}} \times y^{\mathbb{Z}/\ell^{n-b}}.$$

Denote by $\Psi = (f, g)$ then $\Psi(x) = (\ell^a, 0)$ and $\Psi(y) = (0, \ell^b)$. Say that $z = x^h y^i \pmod T$ and $(1 - z) = x^j y^k \pmod T$ where $h, i, j, k \in \mathbb{Z}/\ell^n$; equivalently, one has $\Psi(z) = (\ell^a h, \ell^b i)$ and $\Psi(1 - z) = (\ell^a j, \ell^b k)$. Since $\{z, 1 - z\} = 0$ we deduce that $(hk - ij) \cdot \{x, y\}_T = 0$ and thus

$(hk - ij) = 0 \pmod{\ell^{n-c}}$. Assume that $c \leq a + b$; thus we see that $\ell^{a+b} \cdot (hk - ij) = 0 \pmod{\ell^n}$ and so $f(z)g(1 - z) = f(1 - z)g(z)$. As z was arbitrary, we see that f, g form a C-pair.

Conversely, assume that f, g are a C-pair and assume with no loss that $a \geq b$. Let $z \in K^\times$ be given and say $\Psi(z) = (\ell^a h, \ell^b i)$, $\Psi(1 - z) = (\ell^a j, \ell^b k)$ as above with $h, i, j, k \in \mathbb{Z}/\ell^n$. Since f, g are a C-pair, we see that $\ell^{a+b} \cdot (hk - ij) = 0$. On the other hand, $K_2^M(K)/T = \wedge^2(K^\times/T)/\langle z' \wedge (1 - z') : z' \neq 0, 1 \rangle$. Recall that $\wedge^2(K^\times/T)$ is generated by $x \wedge y$ and has order ℓ^{n-a} . For z as above, one has $z \wedge (1 - z) = (hk - ij) \cdot (x \wedge y)$ so that $\wedge^2(K^\times/T)/\langle z \wedge (1 - z) \rangle \cong \mathbb{Z}/\ell^{n-c}$ where $c \leq a + b$. Varying over all z' , we see that $K_2^M(K)/T \cong \mathbb{Z}/\ell^{n-c}$ where $c \leq a + b$, as required. \square

Remark 6.2. Let $A \leq \mathcal{G}_K^a(n)$ be given and denote by $T = A^\perp$. Proposition 6.1 gives a precise recipe to decide whether or not A is a C-group using the structure of $K_*^M(K)/T$. Indeed, we immediately see that the following conditions are equivalent:

- (1) A is a C-group.
- (2) For all subgroups $A_0 \leq A$ of rank 2, A_0 is a C-group.
- (3) For all subgroups $T_0 \leq K^\times$ such that $T \leq T_0 \leq K^\times$ and K^\times/T_0 has rank 2, $K_*^M(K)/T_0$ satisfies the equivalent conditions of Proposition 6.1.

On the other hand, in the case where $n = 1$, we can provide a direct characterization of C-groups $A \leq \mathcal{G}_K^a(1)$ as follows; see also [Top12] Lemma 2.12. Let $A \leq \mathcal{G}_K^a(1)$ be given and denote by $T = A^\perp$. Then the following are equivalent:

- (1) A is a C-group.
- (2) For all subgroups $T \leq T_0 \leq K^\times$ such that $K^\times/T_0 = \langle x \pmod{T_0}, y \pmod{T_0} \rangle$ has rank 2, one has $\{x, y\}_{T_0} \neq 0$ as an element of $K_2^M(K)/T_0$.
- (3) For all $x, y \in K^\times$ such that $x \pmod{T}, y \pmod{T}$ are \mathbb{Z}/ℓ independent in K^\times/T one has $\{x, y\}_T \neq 0$ as an element of $K_2^M(K)/T$.
- (4) For all $x \in K^\times \setminus T$ one has $\langle 1 - x, x \rangle \pmod{T}$ is cyclic.
- (5) For all $T \leq H \leq K^\times$ and $x \in K^\times \setminus H$ one has $\langle 1 - x, x \rangle \pmod{H}$ is cyclic.
- (6) The canonical map $\wedge^2(K^\times/T) \rightarrow K_2^M(K)/T$ is an isomorphism.
- (7) For all $T \leq H \leq K^\times$, the canonical map $\wedge^2(K^\times/H) \rightarrow K_2^M(K)/H$ is an isomorphism.

Indeed, (1) \Leftrightarrow (2) is Proposition 6.1, while (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (6) \Rightarrow (3) and (5) \Rightarrow (7) \Rightarrow (2) follow immediately from the definitions. In particular, the equivalence of conditions (1) and (6) above give a direct characterization of C-groups $A \leq \mathcal{G}_K^a(1)$ based on the structure of $K_*^M(K)/T$ where $T = A^\perp$.

Remark 6.3. Passing to the limit over $n \in \mathbb{N}$ and using Proposition 6.1, we can obtain a similar K-theoretic method to detect C-pairs in $\mathcal{G}_K^a(\infty)$. Denote by $\widehat{K}_i^M(K)$ the ℓ -adic completion of $K_i^M(K)$ and denote by $\widehat{K} = \widehat{K}_1^M(K)$ the ℓ -adic completion of K^\times , as defined in §1.2. By the universal property of completions one has:

$$\mathcal{G}_K^a(\infty) = \text{Hom}^{\text{cont}}(\widehat{K}/\pm 1, \mathbb{Z}_\ell).$$

Moreover, $\widehat{K}/\text{torsion}$ is in perfect \mathbb{Z}_ℓ -duality with $\mathcal{G}_K^a(\infty)$. Let $f, g \in \mathcal{G}_K^a(\infty)$ be given and consider f, g as homomorphisms $\widehat{K} \rightarrow \mathbb{Z}_\ell$; assume that $\langle f, g \rangle$ is non-cyclic. If $f = \ell^a \cdot f'$ and $g = \ell^b \cdot g'$ then f, g form a C-pair if and only if f', g' form a C-pair. Therefore, we can assume without loss that, first, $\mathcal{G}_K^a(\infty)/\langle f, g \rangle$ is torsion-free and, second, that f, g are independent. In particular $\langle f \pmod{\ell}, g \pmod{\ell} \rangle$ is non-cyclic and f_n, g_n are quasi-independent elements

of $\mathcal{G}_K^a(n)$ both of order \mathbb{Z}/ℓ^n . We denote by $T = \ker f \cap \ker g$ considered as a closed \mathbb{Z}_ℓ -submodule of \widehat{K} . Thus we can find generators x, y for \widehat{K}/T such that $\widehat{K}/T = x^{\mathbb{Z}_\ell} \times y^{\mathbb{Z}_\ell}$ with $(f, g)(x) = (1, 0)$ and $(f, g)(y) = (0, 1)$.

Moreover, denote by $T_n = \ker f_n \cap \ker g_n$, and observe that $\widehat{K}/T = \lim_n K^\times/T_n$. From this we see that $\widehat{K}_2^M(K)/T = \lim_n K_2^M(K)/T_n$ is a cyclic \mathbb{Z}_ℓ -module generated by $\{x, y\}_T$. Recall that f, g form a C-pair if and only if f_n, g_n form a C-pair for all $n \in \mathbb{N}$; we thus deduce from Proposition 6.1 that f, g form a C-pair if and only if $\{x, y\}_T$ has infinite order – i.e. $\widehat{K}_2^M(K)/T = \mathbb{Z}_\ell \cdot \{x, y\}_T \cong \mathbb{Z}_\ell$. Thus, we see that f, g form a C-pair if and only if the canonical map $\widehat{\wedge}^2(\widehat{K}/T) \rightarrow \widehat{K}_2^M(K)/T$ is an isomorphism.

Furthermore, one should remark that Proposition 6.1 allows one to detect valuations using the Milnor K-theory of the field. Indeed, using the results of Part 1, we need to construct $\mathcal{G}_K^a(n)$ along with the C-pairs from Milnor K-theory. First, assume that ℓ is odd and n is finite. Then $\mathcal{G}_K^a(n) = \text{Hom}(K^\times/\ell^n, \mathbb{Z}/\ell^n) = \text{Hom}(K_1^M(K)/\ell^n, \mathbb{Z}/\ell^n)$, and Proposition 6.1 shows how to detect precisely the C-pairs in $\mathcal{G}_K^a(n)$ using $K_*^M(K)/\ell^n$. Thus, one can detect valuations of K using $K_*^M(K)/\ell^N$ when N is sufficiently large with respect to n .

On the other hand, if $\ell = 2$, consider the kernel H of the map:

$$K^\times/2^{n+1} \xrightarrow{x \mapsto x^2} K^\times/2^{n+1}.$$

Then $K^\times/\langle K^{\times 2^n}, -1 \rangle = (K^\times/2^{n+1})/H$. Thus, we can reconstruct $\mathcal{G}_K^a(n)$ from $K^\times/2^{n+1} = K_1^M(K)/2^{n+1}$ and furthermore detect C-pairs using Proposition 6.1 from $K_*^M(K)/2^{n+1}$ and/or $K_*^M(K)/2^n$. Again, one can therefore detect valuations of K using $K_*^M(K)/2^N$ when N is sufficiently large with respect to n .

Lastly, if $n = \infty$ and ℓ is arbitrary, we consider $\widehat{K} = \widehat{K}_1^M(K)$ and observe that the image of -1 in \widehat{K} is either trivial or is the unique element in \widehat{K} whose square is trivial. Thus, we obtain $\mathcal{G}_K^a(\infty) = \text{Hom}(\widehat{K}/\pm 1, \mathbb{Z}_\ell)$ from $\widehat{K}_1^M(K)$. Also, by the discussion above, we obtain the C-pairs in $\mathcal{G}_K^a(\infty)$ from $\widehat{K}_*^M(K)$. Thus, one can detect valuations of K using $\widehat{K}_*^M(K)$.

In particular, if K is a field of characteristic different from ℓ , we obtain a recipe to detect valuations $v \in \mathcal{V}_{K,n}$ using the cup-product structure of the cohomology ring $H^*(K, R_N(*))$ where $N \geq n$ is sufficiently large (as above). In the presence of sufficiently many roots of unity (or if $n = 1, \infty$), this provides a recipe to recover the corresponding maps $H^1(K, R_n(1)) = K^\times/\ell^n \xrightarrow{v} \Gamma_v/\ell^n$ for $v \in \mathcal{V}_{K,n}$ as dual to the inclusion $I_v(n) \hookrightarrow \mathcal{G}_K^a(n)$, resp. $H^1(K, \mathbb{Z}_\ell(1)) = \widehat{K} \xrightarrow{\widehat{v}} \widehat{\Gamma}_v$ as dual to the inclusion $I_v(\infty) \hookrightarrow \mathcal{G}_K(\infty)$.

7. CL SUBGROUPS OF GALOIS GROUPS

Let K be a field of characteristic different from ℓ such that $\mu_\ell \subset K$. Recall that $K(\ell)$ denotes the maximal pro- ℓ Galois extension of K (inside some chosen algebraic closure) and that $\mathcal{G}_K = \text{Gal}(K(\ell)|K)$ denotes the maximal pro- ℓ Galois group of K . Also recall that $\mathcal{G}_K^{a,n}$ denotes the maximal R_n -elementary abelian quotient of \mathcal{G}_K , as introduced in § 1.2 (we reintroduce this notation below). In this section we give a Galois-theoretic characterization of the C-pair property of elements $f, g \in \mathcal{G}_K^a(n)$ under an identification $\mathcal{G}_K^{a,n} \cong \mathcal{G}_K^a(n)$, for fields K such that $\text{char } K \neq \ell$ and $\mu_{2\ell^n} \subset K$, via Kummer theory.

Throughout this section, we will work with a fixed $n \in \overline{\mathbb{N}}$. Let \mathcal{G} be an arbitrary pro- ℓ group. We recall the R_n -central descending series of \mathcal{G} :

$$\mathcal{G}^{(1,n)} = \mathcal{G}, \quad \mathcal{G}^{(m+1,n)} = [\mathcal{G}, \mathcal{G}^{(m,n)}] \cdot (\mathcal{G}^{(m,n)})^{\ell^n}.$$

For simplicity we denote by $\mathcal{G}^{a,n} = \mathcal{G}/\mathcal{G}^{(2,n)}$ and $\mathcal{G}^{c,n} = \mathcal{G}/\mathcal{G}^{(3,n)}$.

We will denote by $H^*(\mathcal{G}) := H_{\text{cont}}^*(\mathcal{G}, R_n)$ throughout this section. Recall, if n is finite, that the short exact sequence:

$$1 \rightarrow \mathbb{Z}/\ell^n \xrightarrow{\ell^n} \mathbb{Z}/\ell^{2n} \rightarrow \mathbb{Z}/\ell^n \rightarrow 1$$

produces the Bockstein homomorphism:

$$\beta : H^1(\mathcal{G}) \rightarrow H^2(\mathcal{G})$$

which is the connecting homomorphism in the associated long exact sequence in cohomology (note the Bockstein map β is taken to be the trivial homomorphism if $n = \infty$).

One has a well-defined R_n -bilinear map:

$$[\bullet, \bullet] : \mathcal{G}^{a,n} \times \mathcal{G}^{a,n} \rightarrow \mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)}$$

defined by $[\sigma, \tau] = \tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}$ where $\tilde{\sigma}$ resp. $\tilde{\tau}$ denotes a lift of σ resp. τ to $\mathcal{G}^{c,n}$. Similarly, one has a map:

$$(\bullet)^\pi : \mathcal{G}^{a,n} \rightarrow \mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)}$$

defined by $\sigma^\pi = \tilde{\sigma}^{\ell^n}$ (here $\sigma^\pi = 0$ if $n = \infty$) where again $\tilde{\sigma}$ denotes some lift of σ to $\mathcal{G}^{c,n}$. The map $\sigma \mapsto \sigma^\pi$ is R_n -linear if $\ell \neq 2$. We will denote $\sigma^\beta = 2 \cdot \sigma^\pi$; thus the map $(\bullet)^\beta : \mathcal{G}^{a,n} \rightarrow \mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)}$ is R_n -linear regardless of ℓ (see [NSW08] Proposition 3.8.3).

Lemma 7.1. *Let \mathcal{G} be a pro- ℓ group. Then*

$$\ker(H^2(\mathcal{G}^{a,n}) \rightarrow H^2(\mathcal{G})) = \ker(H^2(\mathcal{G}^{a,n}) \rightarrow H^2(\mathcal{G}^{c,n})).$$

In particular, let $f, g \in \text{Hom}(\mathcal{G}, R_n) = H^1(\mathcal{G}^{a,n}) = H^1(\mathcal{G}^{c,n}) = H^1(\mathcal{G})$ be given. The following are equivalent:

- (1) $f \cup g = 0 \in H^2(\mathcal{G})$.
- (2) $f \cup g = 0 \in H^2(\mathcal{G}^{c,n})$.

Proof. The fact that

$$\ker(H^2(\mathcal{G}^{a,n}) \rightarrow H^2(\mathcal{G})) \supset \ker(H^2(\mathcal{G}^{a,n}) \rightarrow H^2(\mathcal{G}^{c,n}))$$

is trivial. Assume that $x \in \ker(H^2(\mathcal{G}^{a,n}) \rightarrow H^2(\mathcal{G}))$ and consider the spectral sequence in cohomology associated to the group extension $\mathcal{G} \twoheadrightarrow \mathcal{G}^{a,n}$. Then $x = d_2(\xi)$ for some $\xi \in H^1(\mathcal{G}^{(2,n)})^{\mathcal{G}}$. Observe that the inflation map $H^1(\mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)})^{\mathcal{G}^{c,n}} \rightarrow H^1(\mathcal{G}^{(2,n)})^{\mathcal{G}}$ is an isomorphism. By the functoriality of the spectral sequence associated to a group extension above versus the group extension $\mathcal{G}^{c,n} \twoheadrightarrow \mathcal{G}^{a,n}$, we deduce that $x \in \ker(H^2(\mathcal{G}^{a,n}) \rightarrow H^2(\mathcal{G}^{c,n}))$ as required. \square

Definition 7.2. Let \mathcal{G} be a pro- ℓ group and let $\sigma, \tau \in \mathcal{G}^{a,n}$ be given. We say that σ, τ form a CL-pair provided that:

$$[\sigma, \tau] \in \langle \sigma^\beta, \tau^\beta \rangle.$$

If $\ell \neq 2$ we note that this condition is equivalent to $[\sigma, \tau] \in \langle \sigma^\pi, \tau^\pi \rangle$ as 2 is invertible in R_n . Furthermore, as $(\bullet)^\beta$ is linear and $[\bullet, \bullet]$ is bilinear, if $\langle \sigma', \tau' \rangle = \langle \sigma, \tau \rangle$ and σ, τ form a

CL-pair, then σ', τ' form a CL-pair as well. A subgroup $A \leq \mathcal{G}^{a,n}$ will be called a CL-group provided that any pair of elements $\sigma, \tau \in A$ form a CL-pair.

For a subgroup $A \leq \mathcal{G}^{a,n}$, we denote by $\mathbf{I}^{\text{CL}}(A)$ the subset:

$$\mathbf{I}^{\text{CL}}(A) = \{\sigma \in A : \forall \tau \in A, \sigma, \tau \text{ form a CL-pair.}\}$$

and call $\mathbf{I}^{\text{CL}}(A)$ the CL-center of A . In particular, A is a CL-group if and only if $A = \mathbf{I}^{\text{CL}}(A)$.

Remark 7.3. Let \mathcal{G} be a pro- ℓ group and let $A \leq \mathcal{G}^{a,n}$ be given. Suppose $A = \langle \sigma_i \rangle_i$ is generated by $(\sigma_i)_i$. Note, the fact that $(\sigma_i)_i$ are pairwise CL does not imply that A is CL for a general pro- ℓ group \mathcal{G} . This fact will be a consequence of Theorem 11 in the case where $\mathcal{G} = \mathcal{G}_K$ for a field K of characteristic different from ℓ which contains $\mu_{2\ell^n}$.

Furthermore, suppose A is an arbitrary subgroup of $\mathcal{G}^{a,n}$. We note that $\mathbf{I}^{\text{CL}}(A)$ is not a subgroup of A but merely a subset. It will be a consequence of Theorem 11, in the case where $\mathcal{G} = \mathcal{G}_K$ for a field K as above that $\mathbf{I}^{\text{CL}}(A) \leq A$ is indeed a subgroup which agrees with $\mathbf{I}^{\text{C}}(A)$ of Part 1 under the Kummer identification $\mathcal{G}_K^{a,n} = \text{Hom}(K^\times, R_n(1)) \cong \mathcal{G}_K^a(n)$.

We now recall some basic facts about free presentations of pro- ℓ groups. For a reference, see e.g. [NSW08] Chapter 3.9. Let \mathcal{G} be a pro- ℓ group and $S \rightarrow \mathcal{G}$ a free presentation such that the induced map $S^{a,n} \rightarrow \mathcal{G}^{a,n}$ is an isomorphism, and denote by T the kernel of $S \rightarrow \mathcal{G}$. Say that $(\tilde{\gamma}_i)_{i \in \Lambda}$ is a free generating set of S and denote the image of $\tilde{\gamma}_i$ in $S^{a,n}$ by γ_i – consider γ_i also as an element of $\mathcal{G}^{a,n}$ via the isomorphism above. We furthermore denote by $(x_i)_{i \in \Lambda}$ the R_n -basis for $H^1(S)$ which is dual to $(\gamma_i)_i$ and choose a total ordering for the index set Λ . Every element of $S^{(2,n)}/S^{(3,n)}$ has a unique representation as:

$$\rho = \prod_{i < j} [\gamma_i, \gamma_j]^{a_{ij}(\rho)} \cdot \prod_r (\gamma_r^\pi)^{b_r(\rho)}.$$

As $T \leq S^{(2,n)}$, we can restrict a_{ij} and b_r to homomorphisms $T \rightarrow R_n$. Moreover, the spectral sequence associated to the extension:

$$1 \rightarrow T \rightarrow S \rightarrow \mathcal{G} \rightarrow 1$$

induces an isomorphism:

$$d_2 : H^1(T)^\mathcal{G} \rightarrow H^2(\mathcal{G})$$

since S and T have ℓ -cohomological dimension ≤ 1 and the inflation $H^1(\mathcal{G}) \rightarrow H^1(S)$ is an isomorphism. Thus, we obtain a canonical perfect pairing:

$$(\bullet, \bullet) : H^2(\mathcal{G}) \times \left(\frac{T}{[S, T] \cdot T^{\ell^n}} \right) \rightarrow R_n$$

defined by $(\xi, \rho) = (d_2^{-1}\xi)(\rho)$. We can describe this pairing explicitly using the cup product and Bockstein (see [NSW08] Propositions 3.9.13 and 3.9.14):

- $(x_i \cup x_j, \bullet) = -a_{ij}(\bullet)$, $i < j$.
- $(\beta x_r, \bullet) = -b_r(\bullet)$.

Suppose that K is a field with $\text{char } K \neq \ell$ and $\mu_{2\ell^n} \subset K$, as above. In this context, we will fix, once and for all, an isomorphism of G_K -modules $R_n(1) \cong R_n$ and use it tacitly throughout. Recall the canonical Kummer pairing:

$$\mathcal{G}_K^{a,n} \times K^\times / \ell^n \rightarrow \mathbb{Z}/\ell^n(1) \text{ if } n \neq \infty, \quad \mathcal{G}_K^{a,n} \times \hat{K} \rightarrow \mathbb{Z}_\ell(1) \text{ if } n = \infty.$$

Using our fixed isomorphism $R_n \cong R_n(1)$, we obtain an identification of $\mathcal{G}_K^{a,n}$ with $\mathcal{G}_K^a(n)$. On the other hand, the Merkurjev-Suslin theorem states that $K_2^M(K)/\ell^n \cong H^2(K, \mathbb{Z}/\ell^n(2))$ if $n \neq \infty$ resp. $\widehat{K}_2^M(K) \cong H^2(K, \mathbb{Z}_\ell(2))$ if $n = \infty$. Thus, the cup product $H^1(K, R_n(1)) \otimes H^1(K, R_n(1)) \xrightarrow{\cup} H^2(K, R_n(2))$ is surjective. In particular, the inflation map $H^2(\mathcal{G}_K^{a,n}) \rightarrow H^2(\mathcal{G}_K)$ is surjective as well. This observation will allow us to describe $K_2^M(K)/\ell^n$ resp. $\widehat{K}_2^M(K)$ via the pairings described above.

Proposition 7.4. *Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{\ell^n} \subset K$. Choose a free presentation $S \rightarrow \mathcal{G}_K$ where S is a free pro- ℓ group such that $S^{a,n} \rightarrow \mathcal{G}_K^{a,n}$ is an isomorphism, and denote by R the kernel of the canonical surjective map $S^{c,n} \rightarrow \mathcal{G}_K^{c,n}$. Then one has a canonical pairing:*

$$H^2(\mathcal{G}_K) \times R \rightarrow R_n$$

induced by the free presentation. This pairing is compatible with the canonical pairing:

$$H^2(S^{a,n}) \times S^{(2,n)}/S^{(3,n)} \rightarrow R_n$$

via the inflation map $H^2(S^{(a,n)}) = H^2(\mathcal{G}_K^{a,n}) \rightarrow H^2(\mathcal{G}_K)$ resp. the inclusion $R \hookrightarrow S^{(2,n)}/S^{(3,n)}$.

Proof. Take a minimal free presentation $S \rightarrow \mathcal{G}_K$ as in the proposition and denote by T the kernel of this map. The spectral sequence associated to this extension induces an isomorphism:

$$d_2 : H^1(T)^S \rightarrow H^2(\mathcal{G}_K)$$

so it suffices to show that the canonical map:

$$T/[S, T]T^{\ell^n} \rightarrow T \cdot S^{(3,n)}/S^{(3,n)} = R$$

is an isomorphism; clearly this is a surjective map. Taking R_n -duals of the composition

$$T/[S, T]T^{\ell^n} \rightarrow T \cdot S^{(3,n)}/S^{(3,n)} \hookrightarrow S^{(2,n)}/S^{(3,n)},$$

we obtain the inflation map $H^2(\mathcal{G}_K^{a,n}) \rightarrow H^2(\mathcal{G}_K)$ which is surjective by the Merkurjev-Suslin theorem (see the discussion preceding this proposition). Thus $T/[S, T]T^{\ell^n} \rightarrow S^{(2,n)}/S^{(3,n)}$ is injective by Pontryagin duality so that $T/[S, T]T^{\ell^n} \rightarrow T \cdot S^{(3,n)}/S^{(3,n)} = R$ is injective as well.

The compatibility with the canonical pairing

$$H^2(S^{a,n}) \times S^{(2,n)}/S^{(3,n)} \rightarrow R_n$$

is immediate by the functoriality of the situation, along with our requirement that $S^{a,n} \rightarrow \mathcal{G}_K^{a,n}$ is an isomorphism. \square

Let K be a field whose characteristic is different from ℓ , $n \in \overline{\mathbb{N}}$ and $\mu_{\ell^n} \subset K$, as above. Our fixed isomorphism $R_n(1) \cong R_n$ allows us to explicitly express the Bockstein morphism $\beta : H^1(\mathcal{G}_K, R_n) \rightarrow H^2(\mathcal{G}_K, R_n)$ using Milnor K-theory as follows. First, if $n = \infty$ this map is trivial, so there is nothing to say. Let us assume that $n \in \mathbb{N}$. It seems to be well known that the cup product $\mathbf{1} \cup \delta : H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \otimes \mu_{\ell^n} \rightarrow H^2(\mathcal{G}_K, \mu_{\ell^n})$ is precisely the map $\beta \cup \mathbf{1}$ where δ denotes the canonical map $K^\times \rightarrow H^1(K, \mu_{\ell^n})$ (see [EM11b] Proposition 2.6 for a precise reference). Denote by ω the fixed generator of μ_{ℓ^n} which corresponds to $1 \in \mathbb{Z}/\ell^n$ under our isomorphism. This induces isomorphisms $H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \cong H^1(G_K, \mu_{\ell^n}) \cong K_*^M(K)/\ell^n$ and $H^2(\mathcal{G}_K, \mathbb{Z}/\ell^n) \cong H^2(G_K, \mu_{\ell^n}^{\otimes 2}) \cong K_2^M(K)/\ell^n$. Under these induced isomorphisms, we deduce that the Bockstein morphism $H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \rightarrow H^2(\mathcal{G}_K, \mathbb{Z}/\ell^n)$ corresponds to the

map $K_1^M(K)/\ell^n \rightarrow K_2^M(K)/\ell^n$ defined by $x \mapsto \{x, \omega\}$. Namely, the following diagram commutes:

$$\begin{array}{ccccccc}
K_1^M(K)/\ell^n & \xrightarrow{\cong} & H^1(K, \mu_{\ell^n}) & \xrightarrow{\cong} & H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) & \xlongequal{\quad} & H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \\
\downarrow x \mapsto \{x, \omega\} & & \downarrow \text{induced} & & \downarrow \beta \cup \mu_{\ell^n} & & \downarrow \beta \\
K_2^M(K)/\ell^n & \xrightarrow{\cong} & H^1(K, \mu_{\ell^n}^{\otimes 2}) & \xrightarrow{\cong} & H^2(\mathcal{G}_K, \mu_{\ell^n}) & \xrightarrow{\cong} & H^2(\mathcal{G}_K, \mathbb{Z}/\ell^n)
\end{array}$$

where the isomorphisms on the left are canonical given by the Galois symbol, while the isomorphisms on the right are induced by our fixed isomorphism $\mu_{\ell^n} = \langle \omega \rangle \cong \mathbb{Z}/\ell^n$. We will use this fact in the remainder of the paper without reference to this commutative diagram. Also, we will tacitly use our isomorphism $R_n \cong R_n(1)$ to identify $H^i(\mathcal{G}_K, R_n(j))$ with $H^i(\mathcal{G}_K, R_n)$ whenever we're dealing with a field K which contains μ_{ℓ^n} .

Theorem 11. *Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{2\ell^n} \subset K$. Let $\sigma, \tau \in \mathcal{G}_K^{a,n}$ be given. Consider σ, τ as homomorphisms $\sigma, \tau : K^\times \rightarrow R_n$ via our chosen isomorphism of G_K -modules $R_n(1) \cong R_n$ and the Kummer pairing. Then σ, τ form a CL-pair if and only if they form a C-pair.*

Proof. We can assume that $n \in \mathbb{N}$ is finite for then we obtain the $n = \infty$ case in the limit as in Lemma 6.1 along with the comment at the end of this proof. Also, we can assume that $\langle \sigma, \tau \rangle$ is non-cyclic for otherwise the claim is trivial. Furthermore, we can assume without loss that σ, τ are quasi-independent so that $\langle \sigma, \tau \rangle = \langle \sigma \rangle \times \langle \tau \rangle$. As such, we can choose a minimal generating set $(\sigma_i)_{i \in \Lambda}$ for $\mathcal{G}_K^{a,n}$ so that $1, 2 \in \Lambda$, $\sigma_1^{\ell^a} = \sigma$ and $\sigma_2^{\ell^b} = \tau$. We denote also by $(\tilde{\sigma}_i)_i$ a corresponding (convergent) set of generators for \mathcal{G}_K and $(x_i)_i$ the dual basis for $H^1(\mathcal{G}_K) = K^\times/\ell^n$ associated to $(\sigma_i)_i$. Consider σ_i as homomorphisms $K^\times \rightarrow R_n$ and denote by $H_0 = \ker \sigma_1 \cap \ker \sigma_2$ and $H = \ker \sigma \cap \ker \tau$. Then $H_0 \leq H$, K^\times/H_0 is a free rank 2 \mathbb{Z}/ℓ^n -module generated by x_1, x_2 and $H = \langle H_0, x_1^{\ell^{n-a}}, x_2^{\ell^{n-b}} \rangle$.

Assume first that σ, τ form a CL-pair. Denote by $A = \langle \sigma_1, \sigma_2 \rangle$ and $A^c = \langle \tilde{\sigma}_1, \tilde{\sigma}_2 \rangle \bmod \mathcal{G}_K^{(3,n)} \leq \mathcal{G}_K^{c,n}$. Consider the following commutative diagram:

$$\begin{array}{ccc}
H^1(\mathcal{G}_K^{a,n}) \times H^1(\mathcal{G}_K^{a,n}) & \xrightarrow{\text{info}\cup} & H^2(\mathcal{G}_K^{c,n}) \\
\downarrow \text{res} \times \text{res} & & \downarrow \text{res} \\
H^1(A) \times H^1(A) & \xrightarrow{\text{info}\cup} & H^2(A^c)
\end{array}$$

Via our Kummer identification $H^1(\mathcal{G}_K^{a,n}) \cong K^\times/\ell^n$, the restriction map $\text{res} : H^1(\mathcal{G}_K^{a,n}) \rightarrow H^1(A)$ corresponds precisely to the projection $K^\times/\ell^n \rightarrow K^\times/H_0$. By Lemma 7.1, the top map factors via $K_2^M(K)/\ell^n$ and therefore the bottom map factors via $K_2^M(K)/H_0$. Let F be the free pro- ℓ group on generators $\tilde{\gamma}_1, \tilde{\gamma}_2$, and consider the surjective map $F \rightarrow A^c$ defined by $\tilde{\gamma}_i \mapsto \tilde{\sigma}_i \bmod \mathcal{G}_K^{(3,n)}$; denote by T the kernel this presentation $F \rightarrow A^c$ and γ_i the image of $\tilde{\gamma}_i$ in $F^{a,n}$. As $\sigma_1^{\ell^a}, \sigma_2^{\ell^b}$ form a CL-pair, we see that $T \cdot F^{(3,c)}/F^{(3,c)} = T/F^{(3,c)}$ contains an element of the form:

$$\rho = [\gamma_1, \gamma_2]^{\ell^{a+b}} \cdot (\gamma_1^\beta)^{c_1 \cdot \ell^a} \cdot (\gamma_2^\beta)^{c_2 \cdot \ell^b}.$$

We recall the pairing associated to the presentation $F \rightarrow A^c$,

$$(\bullet, \bullet) : H^2(A^c) \times \left(\frac{T}{[F, T] \cdot T^{\ell^n}} \right) \rightarrow \mathbb{Z}/\ell^n,$$

satisfies $(x_1 \cup x_2, \rho) = -\ell^{a+b}$ and thus $K_2^M(K)/H_0 = \langle \{x_1, x_2\}_{H_0} \rangle$ has order ℓ^{n-c_0} for some c_0 such that $c_0 \leq a+b$. On the other hand, since $H = \langle H_0, x_1^{\ell^a}, x_2^{\ell^b} \rangle$, we see that $K_2^M(K)/H = \langle \{x_1, x_2\}_{H_0} \rangle / \langle \{x_1^{\ell^{n-a}}, x_2\}_{H_0}, \{x_1, x_2^{\ell^{n-b}}\}_{H_0} \rangle$. Thus, $K_2^M(K)/H$ has order ℓ^{n-c} where $\max(a, b, c_0) = c \leq a+b$. Therefore σ, τ form a C-pair by the K-theoretic criterion (Proposition 6.1).

Conversely, assume that σ, τ form a C-pair. Let $S \rightarrow \mathcal{G}_K$ be a minimal free presentation associated to the minimal generating set $(\tilde{\sigma}_i)_i$ – i.e. S is free on $(\tilde{\gamma}_i)_i$ and $\tilde{\gamma}_i \mapsto \tilde{\sigma}_i$ under the map $S \rightarrow \mathcal{G}_K$ so that $S^{a,n} \rightarrow \mathcal{G}_K^{a,n}$ is an isomorphism; we also denote by γ_i the image of $\tilde{\gamma}_i$ in $S^{a,n}$. Furthermore, we denote by R the kernel of the induced surjective map $S^{c,n} \rightarrow \mathcal{G}_K^{c,n}$. Then $K_2^M(K)/H$ is a rank-1 quotient of $K_2^M(K)/\ell^n$ which corresponds via the pairing of Proposition 7.4 to a rank-1 subgroup of R , generated by, say

$$\rho = \prod_{i < j} [\gamma_i, \gamma_j]^{a_{ij}} \cdot \prod_r (\gamma_r^\pi)^{b_r}.$$

As $x_i \in H$ for all $i \neq 1, 2$ we deduce that $\rho = [\gamma_1, \gamma_2]^{a_{12}} \cdot (\gamma_1^\pi)^{b_1} \cdot (\gamma_2^\pi)^{b_2}$. Recall that ω denotes the generator of μ_{ℓ^n} which corresponds to $1 \in \mathbb{Z}/\ell^n$. Write $\omega = x_1^{-2j} x_2^{2k} \pmod{H}$ (recall that $\mu_{2\ell^n} \subset K$ so that ω is indeed a square in K^\times) then:

- $(\{x_1, x_2\}_H, \rho) = -a_{12}$
- $(\{x_1, \omega\}_H, \rho) = 2k(\{x_1, x_2\}_H, \rho) = -2ka_{12} = -b_1.$
- $(\{x_2, \omega\}_H, \rho) = 2j(\{x_1, x_2\}_H, \rho) = -2ja_{12} = -b_2.$

where (\bullet, \bullet) denotes the pairing of Proposition 7.4, identifying $K_2^M(K)/H$ with the corresponding quotient of $H^2(\mathcal{G}_K)$. Thus:

$$\rho = ([\gamma_1, \gamma_2](\gamma_1^\beta)^k (\gamma_2^\beta)^j)^{a_{12}}.$$

Since $\langle \rho \rangle$ is in a perfect pairing with $K_2^M(K)/H = \langle \{x_1, x_2\}_H \rangle$, we deduce from the K-theoretic criterion (Proposition 6.1) that $a_{12} \in \mathbb{Z}/\ell^n$ has (additive) order ℓ^{n-c} where $c \leq a+b$. In particular, $\ell^{a+b} = a_{12} \cdot t$ for some t so that there exists an element of R of the form:

$$\rho^t = [\gamma_1, \gamma_2]^{\ell^{a+b}} (\gamma_1^\beta)^{k\ell^{a+b}} (\gamma_2^\beta)^{j\ell^{a+b}} = [\gamma_1^{\ell^a}, \gamma_2^{\ell^b}] \cdot ((\gamma_1^{\ell^a})^\beta)^{k\ell^b} ((\gamma_2^{\ell^b})^\beta)^{j\ell^a}$$

and in particular we deduce that $[\sigma, \tau] \in \langle \sigma^\beta, \tau^\beta \rangle$ as required. To conclude the theorem in the case where $n = \infty$, we note that j, k above would have been zero provided that $\mu_{\ell^\infty} \subset K$. \square

Remark 7.5. As an immediate corollary of Theorem 11 we deduce the following. Given $(\sigma_i)_i \in \mathcal{G}_K^{a,n}$ which are pairwise CL, then any pair $\sigma, \tau \in \langle \sigma_i \rangle_i$ form a CL-pair. We note that this doesn't follow immediately from the definition of CL-pairs. We also deduce that, for $A \leq \mathcal{G}_K^{a,n}$, the subset $\mathbf{I}^{\text{CL}}(A) \subset A$ is indeed a subgroup which corresponds to $\mathbf{I}^{\text{C}}(A)$ as defined in Part 1 via the identification $\mathcal{G}_K^{a,n} \cong \mathcal{G}_K^a(n)$.

Remark 7.6. Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{2\ell} \subset K$ and let $A \leq \mathcal{G}_K^{a,1}$ be given. Using Remark 6.2, we can now give an alternative definition for $\mathbf{I}^{\text{CL}}(A)$. Namely, in this remark we will show that:

$$\mathbf{I}^{\text{CL}}(A) = \{\sigma \in A : \forall \tau \in A, [\sigma, \tau] \in A^\beta\} =: I.$$

Observe that $\mathbf{I}^{\text{CL}}(A) \leq I$ by definition and so it suffices to prove that $I \leq \mathbf{I}^{\text{CL}}(A)$. We will identify $\mathcal{G}_K^a(1)$ and $\mathcal{G}_K^{a,1}$ via Kummer theory, as well as the notions of C-pairs resp. CL-pairs using Theorem 11.

Denote by $T = A^\perp$ and $H = I^\perp$ and suppose that $T \leq G \leq H \leq K^\times$ is given such that H/G is cyclic. We will show that $\text{Hom}(K^\times/G, \mathbb{Z}/\ell) \leq A$ is a C-group, therefore proving that $\langle I, f \rangle$ is a C-group for all $f \in A$. This would immediately imply that $I \leq \mathbf{I}^{\text{CL}}(A)$ as required above.

Let $x_1 \in K^\times \setminus H$ and $x_2 \in K^\times \setminus T$ be given such that $x_1 \bmod T$ and $x_2 \bmod T$ are \mathbb{Z}/ℓ -independent. We can therefore complete x_1, x_2 to a \mathbb{Z}/ℓ -basis $(x_i)_i$ for K^\times/T , with dual basis $(\sigma_i)_i$ for A , in such a way so that $\sigma_1 \in I$. Thus, we see that $[\sigma_1, \sigma_2] \in \langle \sigma_i^\beta \rangle_i$ by the definition of I . Arguing as in the first part of the proof of Theorem 11, we will deduce that $\{x_1, x_2\}_T \neq 0$. Indeed, choose lifts (continuously) $\sigma_i^c \in \mathcal{G}_K^{c,1}$ for σ_i , denote by $A^c = \langle \sigma_i^c \rangle_i$, F the free pro- ℓ -group on $(\gamma_i)_i$, and $F \twoheadrightarrow A^c$ a free presentation sending γ_i to σ_i^c . Denote by R the kernel of $F \rightarrow A^c$; thus $R/F^{(3,1)}$ contains an element of the form:

$$\rho = [\gamma_1, \gamma_2] \cdot \prod_r (\gamma_i^\beta)^{b_r}.$$

And, as in the proof of Theorem 11 we see that $(x_1 \cup x_2, \rho) = 1$ where (\bullet, \bullet) is the pairing of Proposition 7.4. Thus $\{x_1, x_2\}_T \neq 0$ since the cup product $H^1(A, \mathbb{Z}/\ell) \times H^1(A, \mathbb{Z}/\ell) = H^1(A^c, \mathbb{Z}/\ell) \times H^1(A^c, \mathbb{Z}/\ell) \rightarrow H^2(A^c, \mathbb{Z}/\ell)$ factors through $K_2^M(K)/T$.

Now suppose that $x \in K^\times \setminus G$ is given and consider $1 - x \in K^\times$. If either $x \notin H$ or $1 - x \notin H$, we deduce from the argument above that $\langle x, 1 - x \rangle \bmod T$ is cyclic since $\{x, 1 - x\}_T = 0$ (and thus $x \bmod T, (1 - x) \bmod T$ cannot be \mathbb{Z}/ℓ -independent); therefore $\langle x, 1 - x \rangle \bmod G$ is cyclic as well. On the other hand, if both $x, 1 - x \in H$, then $\langle x, 1 - x \rangle \bmod G$ is cyclic since H/G is cyclic. Thus, G satisfies condition (4) of Remark 6.2 which proves that $\text{Hom}(K^\times/G, \mathbb{Z}/\ell)$ is a C-group.

Remark 7.7. Let (K, v) be a valued field such that $\text{char } K \neq \ell$ and $\mu_{2\ell^n} \subset K$. Recall that we denote by $K^{a,n} = K(\sqrt[n]{K})$ and we define the minimized decomposition/inertia subgroups of v to be:

$$D_v^n := \text{Gal}(K^{a,n} | K(\sqrt[\ell]{1 + \mathfrak{m}_v})), \quad \text{and} \quad I_v^n := \text{Gal}(K^{a,n} | K(\sqrt[\ell]{\mathcal{O}_v^\times})).$$

It turns out that these minimized decomposition and inertia subgroups behave very much like regular inertia and decomposition groups when it comes to the Galois group $\mathcal{G}_K^{a,c}$, regardless of $\text{char } k(v)$. In particular, we will show the following. Let $\sigma, \tau \in D_v^n$ be given and consider them as homomorphisms $K^\times \rightarrow R_n$ via Kummer theory.

- (1) If $\sigma, \tau \in I_v^n$ then $[\sigma, \tau] = 0$.
- (2) If $\sigma \in I_v^n$ and $\tau \in D_v^n$ then $[\sigma, \tau] \in \langle \sigma^\beta \rangle$; more precisely, if $\tau(\omega) = 2a \in R_n$ then $[\sigma, \tau] = -a \cdot \sigma^\beta = -2a \cdot \sigma^\pi$.

In order to prove this claim, it suffices to assume that σ, τ are actually R_n -independent. Choose a minimal generating set $(\sigma_i)_i$ such that $\sigma_1 = \sigma$ and $\sigma_2 = \tau$ with corresponding dual basis $(x_i)_i$ for $H^1(K, R_n(1)) \cong H^1(\mathcal{G}_K^{a,n}, R_n)$. We then choose a corresponding free presentation $S \rightarrow \mathcal{G}_K$ and use the same notation as in the second part of the proof of Theorem 11 – in particular, R denotes the kernel of $S^{c,n} \rightarrow \mathcal{G}_K^{c,n}$. We see that it suffices to prove the stronger part of (2) since, if $\tau = \sigma_2 \in I_v^n$, we see that $\sigma_2(\omega) = 0$; in both cases, we see that $\sigma_1(\omega) = 0$ since $\omega \in \mathcal{O}_v^\times$. Suppose, then, that $\sigma_2(\omega) = 2a$ and denote by $H = \ker \sigma_1 \cap \ker \sigma_2$. Therefore, $\omega = x_1^{\sigma_1(\omega)} \cdot x_2^{\sigma_2(\omega)} \bmod H = x_2^{2a} \bmod H$. In light of Theorem 11 and Lemma 3.11, we see that R contains an element of the form

$$\rho = [\gamma_1, \gamma_2] \cdot (\gamma_1^\beta)^{c_1} \cdot (\gamma_2^\beta)^{c_2},$$

and arguing as in the proof of Theorem 11 we see that $\langle \rho \rangle$ is in perfect duality with $K_2^M(K)/H$ via the pairing of Proposition 7.4; namely, $(\{x_1, x_2\}, \rho) = 1$ and $(\beta x_i, \rho) = 2c_i$. Therefore, we see that $2c_1 = (\beta x_1, \rho) = (\{x_1, \omega\}, \rho) = 2a(\{x_1, x_2\}, \rho) = 2a$ and $2c_2 = (\beta x_2, \rho) = (\{x_2, \omega\}, \rho) = 2a(\{x_2, x_2\}, \rho) = 0$. In particular, R contains an element ρ of the form $[\gamma_1, \gamma_2] \cdot (\gamma_1^\beta)^a$. Thus, we see that $[\sigma_1, \sigma_2] = -a \cdot \sigma_1^\beta$, as required.

Choose a minimal generating set $(\eta_i)_i$ for I_v^n and complete it to a minimal generating set $(\eta_i)_i \cup (\tau_j)_j$ for D_v^n . Choose (continuously) lifts $\eta_i^c \in \mathcal{G}_K^{c,n}$ and $\tau_j^c \in \mathcal{G}_K^{c,n}$ for η_i and τ_j . Denote by $I^c = \langle \eta_i^c \rangle$ and $D^c = \langle \eta_i^c, \tau_j^c \rangle$. We deduce from the discussion above that I^c is an **abelian normal subgroup** of D^c . Moreover, by construction we see that $D^c \cap (\mathcal{G}_K^{c,n})^{(2,n)} = (D^c)^{(2,n)}$, $I^c \cap (\mathcal{G}_K^{c,n})^{(2,n)} = (I^c)^{(2,n)} = I^c \cap (D^c)^{(2,n)}$, the image of I^c in $\mathcal{G}_K^{a,n}$ is I_v^n , the image of D^c in $\mathcal{G}_K^{a,n}$ is D_v^n and $(D^c/I^c)^{a,n} = \mathcal{G}_{k(v)}^{a,n}$.

8. PROOF OF THEOREM 1

We restate Theorem 1 using the notation of the paper.

Theorem 12. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{2\ell^N} \subset K$.*

- (1) *Let $D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation v of K such that $D \leq D_v^n$ and $D/D \cap I_v^n$ is cyclic if and only if there exists a CL-group $D' \leq \mathcal{G}_K^{a,N}$ such that $D'_n = D$.*
- (2) *Let $I \leq D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v^n$ and $D = D_v^n$ if and only if the following hold:*
 - (a) *There exist $D' \leq \mathcal{G}_K^{a,N}$ such that $(\mathbf{I}^{\text{CL}}(D'))_n = I$ and $D'_n = D$.*
 - (b) *$I \leq D \leq \mathcal{G}_K^{a,n}$ are maximal with this property – i.e. if $D \leq E \leq \mathcal{G}_K^{a,n}$ and $E' \leq \mathcal{G}_K^{a,N}$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^{\text{CL}}(E'))_n$, then $D = E$ and $I = (\mathbf{I}^{\text{CL}}(E'))_n$.*
 - (c) *$\mathbf{I}^{\text{CL}}(D) \neq D$ (i.e. D is not a CL-group).*

Proof. Using our isomorphism $R_N \cong R_N(1)$, along with the observation that $-1 \in K^{\times \ell^N}$, we obtain isomorphisms using Kummer theory, $\phi_m : \mathcal{G}_K^{a,m} \cong \mathcal{G}_K^a(m)$ for all $m \leq N$ which are compatible with the projections $\mathcal{G}_K^{a,M} \rightarrow \mathcal{G}_K^{a,m}$ resp. $\mathcal{G}_K^a(M) \rightarrow \mathcal{G}_K^a(m)$ for $m \leq M \leq N$. Furthermore, let $H \leq K^\times$ be given. Via these isomorphisms, the subgroup $\text{Gal}(K^{a,m}|K(\sqrt[m]{H}))$ of $\mathcal{G}_K^{a,m}$ is mapped isomorphically onto $\text{Hom}(K^\times/H, R_m) \leq \mathcal{G}_K^a(m)$. Thus, in particular, I_v^m is mapped isomorphically onto $I_v(m)$ and D_v^m is mapped isomorphically onto $D_v(m)$ for all valuations v of K and $m \leq N$. By Theorem 11, these isomorphisms send CL-pairs to C-pairs and in particular, $\mathbf{I}^{\text{CL}}(A)$ is sent to $\mathbf{I}^{\text{C}}(\phi_m A)$ for $A \leq \mathcal{G}_K^{a,m}$. Now, in light of these compatible identifications, we immediately see the first part of Theorem 12 follows from Proposition 4.5, and the second part from Theorem 6. \square

Part 3. Applications

In this section we provide two applications using the theory above. We show how to detect the decomposition and inertia subgroups of valuations $v \in \mathcal{V}_{K,n}$ whose residue characteristic is different from ℓ , using purely group theoretical methods. We also show an application towards the structure of maximal pro- ℓ Galois groups.

9. HILBERT DECOMPOSITION THEORY

Let (K, v) be a valued field such that $\text{char } K \neq \ell$ and $\mu_{\ell^n} \subset K$. Pick a prolongation v' of v to $K^{a,n} = K(\sqrt[n]{K})$. We denote by $Z_v^n = Z_{v'|v}$ resp. $T_v^n = T_{v'|v}$ the decomposition and inertia subgroups of $v'|v$ inside $\mathcal{G}_K^{a,n} = \text{Gal}(K^{a,n}|K)$. Note that as $\mathcal{G}_K^{a,n}$ is abelian, the subgroups $T_v^n \leq Z_v^n$ are independent of choice of prolongation v' .

In fact, if $\text{char } k(v) \neq \ell$, we can explicitly describe these subgroups via the Kummer pairing $K^\times / \ell^n \times \mathcal{G}_K^{a,n} \rightarrow \mu_{\ell^n}$ (resp. $\widehat{K} \times \mathcal{G}_K^{a,\infty} \rightarrow \mu_{\ell^\infty}$) – see Proposition 9.1. Before we prove this proposition, we first review some basic facts from Hilbert decomposition theory for a valued field (K, v) such that $\text{char } k(v) \neq \ell$ and $\mu_\ell \subset K$.

Assume, then, that $\text{char } k(v) \neq \ell$, let $L|K$ be an arbitrary pro- ℓ Galois extension ($K \subset L \subset K(\ell)$) and pick a prolongation w of v to L . We denote by $T_{w|v}$ resp. $Z_{w|v}$ the inertia resp. decomposition subgroups of $w|v$ in $\text{Gal}(L|K)$. One has a canonical short exact sequence:

$$1 \rightarrow T_{w|v} \rightarrow Z_{w|v} \rightarrow \text{Gal}(k(w)|k(v)) \rightarrow 1;$$

recall that this short exact sequence is split if $L = K(\ell)$ and that $k(w) = k(v)(\ell)$ in this case. Moreover, we have a perfect pairing which is compatible with the action of $\text{Gal}(k(w)|k(v))$ on $T_{w|v}$:

$$T_{w|v} \times (\Gamma_w / \Gamma_v) \rightarrow \mu_{\ell^\infty}(k(w)) = \mu_{\ell^\infty} \cap k(v)^\times$$

defined by $(\sigma, w(x)) \mapsto \overline{\sigma x / x}$ where $y \mapsto \bar{y}$ is the canonical map $\mathcal{O}_w^\times \twoheadrightarrow k(w)^\times$. To simplify the notation, we denote by $\mu_{\ell^v} := \mu_{\ell^\infty}(k(v)) = \mu_{\ell^\infty} \cap k(v)^\times$. This pairing is compatible with the action of $\text{Gal}(k(w)|k(v))$ on $T_{w|v}$; in particular $\text{Gal}(k(w)|k(v))$ acts on $T_{w|v}$ via the cyclotomic character $\text{Gal}(k(w)|k(v)) \twoheadrightarrow \text{Gal}(k(v)(\mu_{\ell^w})|k(v))$.

If we have a tower of pro- ℓ Galois extensions of valued fields: $(K, v) \subset (L, w) \subset (F, w')$ then:

- $T_{w'|v}|_L = T_{w|v}$ and $Z_{w'|v}|_L = Z_{w|v}$.
- $T_{w'|v} \cap \text{Gal}(F|L) = T_{w'|w}$ and $Z_{w'|v} \cap \text{Gal}(F|L) = Z_{w'|w}$.

Moreover, the corresponding pairings described above are compatible. I.e. the following diagram is commutative in the natural sense:

$$\begin{array}{ccc} T_{w'|v} \times (\Gamma_{w'} / \Gamma_v) & \longrightarrow & \mu_{\ell^{w'}} \\ \downarrow & \uparrow & \uparrow \\ T_{w|v} \times (\Gamma_w / \Gamma_v) & \longrightarrow & \mu_{\ell^w} \end{array}$$

Moreover, the two pairings are compatible with the action of $\text{Gal}(k(w')|k(v))$ on $T_{w'|v}$ resp. $\text{Gal}(k(w)|k(v))$ on $T_{w|v}$. I.e. the surjective map $T_{w'|v} \twoheadrightarrow T_{w|v}$ is $(\text{Gal}(k(w')|k(v)))$ -equivariant; here $\text{Gal}(k(w')|k(v))$ acts on $T_{w|v}$ via the projection $\text{Gal}(k(w')|k(v))$ onto $\text{Gal}(k(w)|k(v))$.

The proof of the following proposition can be found in [Pop10b] Fact 2.1 in the $n = \infty$ case and in [Pop12] in the $n = 1$ case, but is explicitly stated for valuations v such that $\text{char } k(v) \neq \ell$. It turns out that the same proof works, at least in one direction, even if $\text{char } k(v) = \ell$ and we summarize this in the proposition below.

Proposition 9.1. *Let (K, v) be a valued field such that $\text{char } K \neq \ell$ and $\mu_{\ell^n} \subset K$. Recall that $D_v^n = \text{Gal}(K^{a,n}|K(\sqrt[n]{1 + \mathfrak{m}_v}))$ and $I_v^n = \text{Gal}(K^{a,n}|K(\sqrt[n]{\mathcal{O}_v^\times}))$. Then $D_v^n \leq Z_v^n$ and $I_v^n \leq T_v^n$. If furthermore $\text{char } k(v) \neq \ell$ then $D_v^n = Z_v^n$ and $I_v^n = T_v^n$.*

Proof. The $n = \infty$ case follows easily from the $n \in \mathbb{N}$ case. Thus, we prove the claim for $n \in \mathbb{N}$.

Suppose $a \in K^\times$ is such that $\sqrt[n]{a} \in (K^{a,n})^{Z_v^n}$ and denote by w a prolongation of v to $(K^{a,n})^{Z_v^n}$. Since $\Gamma_w = \Gamma_v$, there exists $y \in K^\times$ such that $v(a) = \ell^n \cdot v(y)$. Moreover, as $k(v) = k(w)$, there exists $z \in \mathcal{O}_v^\times$ such that $\sqrt[n]{a}/y \in z \cdot (1 + \mathfrak{m}_w)$. Namely, $a/(yz)^{\ell^n} \in (1 + \mathfrak{m}_v)$ so that $\sqrt[n]{a} \in K(\sqrt[n]{1 + \mathfrak{m}_v})$. Thus, $D_v^n \leq Z_v^n$ since $(K^{a,n})^{Z_v^n} \subset K(\sqrt[n]{1 + \mathfrak{m}_v})$. The proof that $(K^{a,n})^{T_v^n} \subset K(\sqrt[n]{\mathcal{O}_v^\times})$ is similar.

Assume furthermore that $\text{char } k(v) \neq \ell$. Let (K^Z, v) be some Henselization of (K, v) ; recall that $K^Z \cap K^{a,n} = (K^{a,n})^{Z_v^n}$. Let $a \in 1 + \mathfrak{m}_v$ be given. The polynomial $X^{\ell^n} - a$ reduces mod \mathfrak{m}_v to $X^{\ell^n} - 1$. Since $\text{char } k(v) \neq \ell$ one has $\mu_{\ell^n} \subset k(v)$ and this polynomial has ℓ^n unique roots in $k(v)$. Namely, $X^{\ell^n} - a$ has a root in $K^Z \cap K^{a,n} = (K^{a,n})^{Z_v^n}$. By Hensel's lemma, $K(\sqrt[n]{1 + \mathfrak{m}_v}) \subset (K^{a,n})^{Z_v^n}$. The proof that $K(\sqrt[n]{\mathcal{O}_v^\times}) \subset (K^{a,n})^{T_v^n}$ is similar. \square

Remark 9.2. If $\text{char } K \neq \ell$, $\mu_\ell \subset K$ and $\text{char } k(v) = \ell$, one has $I_v^1 \leq D_v^1 \leq T_v^1$. This can be deduced in a similar way to [Pop10] Lemma 2.3(2); we sketch the argument below. Denote by $\lambda = \omega - 1 \in K$ where $\omega = \omega_\ell$ is our fixed generator of μ_ℓ and recall that $v(\lambda) > 0$ since $\text{char } k(v) = \ell$. Let $u \in \mathcal{O}_v^\times$ be given and set $u' = \lambda^\ell \cdot u + 1 \in 1 + \mathfrak{m}_v$. Then the extension of K corresponding to the equation $X^\ell - u'$ is precisely the same as the extension of K corresponding to the equation $Y^\ell - Y + \lambda \cdot f(Y) = u$ for some (explicit) polynomial $f(Y)$ – this is done by making the change of variables $X = \lambda Y + 1$. On the other hand, the maximal (\mathbb{Z}/ℓ) -elementary abelian Galois extension of $k(v)$ is the extension of $k(v)$ generated by roots of polynomials of the form $X^\ell - X = \bar{u}$ for $\bar{u} \in k(v)$. Thus, the maximal (\mathbb{Z}/ℓ) -elementary abelian Galois extension of $k(v)$ is a subextension of the residue extension corresponding to $K(\sqrt[\ell]{1 + \mathfrak{m}_v})|K$. This immediately implies that $I_v^1 \leq D_v^1 \leq T_v^1$ as required.

10. PROOF OF THEOREM 2

Let us first recall some notation from the introduction. We denote by $\mathcal{V}'_{K,n}$ the collection of (possibly trivial) valuations v of K such that:

- (1) $\text{char } k(v) \neq \ell$.
- (2) Γ_v contains no non-trivial ℓ -divisible convex subgroups.
- (3) v is maximal among all valuations w such that $\text{char } k(w) \neq \ell$, $D_v^n = D_w^n$ and Γ_w contains no non-trivial ℓ -divisible convex subgroups; i.e. for all refinements w of v such that $\text{char } k(w) \neq \ell$ and $D_w^n = D_v^n$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I_w^n = I_v^n$.
- (4) $\mathcal{G}_{k(v)}^{a,n}$ is non-cyclic.

We observe that $\mathcal{V}_{K,n} = \mathcal{V}'_{K,n}$ whenever $\ell \neq \text{char } K > 0$; for an arbitrary field K , one has:

$$\{v \in \mathcal{V}_{K,n} : \text{char } k(v) \neq \ell\} \subset \mathcal{V}'_{K,n}.$$

We now restate Theorem 2 using the notation of the paper.

Theorem 13. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that $\text{char } K \neq \ell$ and $\mu_{2\ell^N} \subset K$.*

- (1) *Let $D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L = (K^{a,n})^D$. Then there exists a valuation v of K such that $\text{char } k(v) \neq \ell$, $D \leq Z_v^n$ and $D/D \cap T_v^n$ is cyclic if and only if there exists a CL-group $D' \leq \mathcal{G}_L^{a,N}$ such that $(D'_n)_K = D$.*
- (2) *Assume that $\mathbf{I}^{\text{CL}}(\mathcal{G}_K^{a,n}) \neq \mathcal{G}_K^{a,n}$ and consider $(\mathbf{I}^{\text{CL}}(\mathcal{G}_K^{a,N}))_n =: T$. Then there exists a (possibly trivial) valuation $v \in \mathcal{V}_{K,n}$ such that $\text{char } k(v) \neq \ell$, $T = T_v^n$ and $\mathcal{G}_K^{a,n} = Z_v^n$.*

- (3) Let $v \in \mathcal{V}_{K,n}$ be given and denote by $I := I_v^n \leq D_v^n =: D$, $L = (K^{a,n})^D$. Then $\text{char } k(v) \neq \ell$ if and only if there exist $I' \leq D' \leq \mathcal{G}_L^{a,N}$ such that:
- (a) $I' \leq \mathbf{I}^{\text{CL}}(D')$.
 - (b) $(I'_n)_K = I$ and $(D'_n)_K = D$.
- Moreover, if these equivalent conditions hold then $I = I_v^n = T_v^n$ and $D = D_v^n = Z_v^n$.
- (4) Let $I \leq D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L = (K^{a,n})^D$. Then there exists a valuation $v \in \mathcal{V}'_{K,n}$ such that $I = T_v^n$ and $D = Z_v^n$ if and only if the following hold:
- (a) There exist $D' \leq \mathcal{G}_L^{a,N}$ such that $((\mathbf{I}^{\text{CL}}(D'))_n)_K = I$ and $(D'_n)_K = D$.
 - (b) $I \leq D \leq \mathcal{G}_K^{a,n}$ are maximal with this property – i.e. if $D \leq E \leq \mathcal{G}_K^{a,n}$ and $E' \leq \mathcal{G}_L^{a,N}$ is given such that $(E'_n)_K = E$ and $I \leq ((\mathbf{I}^{\text{CL}}(E'))_n)_K$, then $D = E$ and $I = ((\mathbf{I}^{\text{CL}}(E'))_n)_K$.
 - (c) $\mathbf{I}^{\text{CL}}(D) \neq D$ (i.e. D is not a CL-group).

Proof. Using our chosen isomorphism $R_n \cong R_n(1)$, we obtain the same compatible isomorphisms $\mathcal{G}_K^{a,m} \cong \mathcal{G}_K^a(m)$ for all $m \leq N$, as in the proof of Theorem 1. We furthermore obtain similar isomorphisms $\mathcal{G}_F^{a,m} \cong \mathcal{G}_F^a(m)$ for all field extensions $F|K$, in a compatible way with the isomorphisms $\mathcal{G}_K^{a,m} \cong \mathcal{G}_K^a(m)$. We will tacitly use these compatible isomorphisms and also the equivalence of “C-pairs” and “CL-pairs.”

We will further make use of the following observation. Suppose $D \leq Z_v^n$ and denote by $L = (K^{a,n})^D$. Choose a prolongation w of v to L . Then the image of the canonical map $Z_w^n \rightarrow Z_v^n$ has image D . Moreover, the image of $T_w^n \rightarrow T_v^n$ is precisely $D \cap T_v^n$. In particular, we see that the image of the canonical map $Z_w^N \rightarrow Z_v^N$ is D and the image of $T_w^N \rightarrow T_v^N$ is $D \cap T_v^N$. Furthermore, we recall that by Proposition 9.1, $I_v^m = T_v^m$ and $D_v^m = Z_v^m$ whenever $\text{char } k(v) \neq \ell$ and $m \leq N$.

Proof of (1): Let $D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L = (K^{a,n})^D$. Assume first that there exists a CL-group $D' \leq \mathcal{G}_L^{a,N}$ such that $(D'_n)_K = D$. By Theorem 9, there exists a valutive subgroup $I \leq D$ such that $\text{char } k(v_I) \neq \ell$, $D \leq D_{v_I}^n$, and D/I is cyclic.

Conversely, assume that there exists a valuation v such that $\text{char } k(v) \neq \ell$, $D \leq Z_v^n$ and $D/D \cap T_v^n$ is cyclic. Denote by $I = D \cap T_v^n$ and choose $f \in D$ such that $D = \langle I, f \rangle$. Choose a prolongation v' of v to L . By the observation above, along with the discussion of §9, there exists $f' \in Z_{v'}^N$ such that $(f'_n)_K = f$. Moreover, I is contained in the image of the canonical map $T_{v'}^N \rightarrow T_v^N$; we denote by I' the pre-image of I in $T_{v'}^N$. By Lemma 3.11 and/or the discussion of §9, $D' = \langle I', f' \rangle$ is a CL-group and $(D'_n)_K = D$.

Proof of (2): Denote by $I = (\mathbf{I}^{\text{CL}}(\mathcal{G}_K^{a,N}))_n$. By Proposition 4.6, $I = I_{v_I}(n)$ and $\mathcal{G}_K^{a,n} = D_{v_I}(n)$. Moreover, by Theorem 10, $\text{char } k(v_I) \neq \ell$, as needed.

Proof of (3): Let $v \in \mathcal{V}_{K,n}$ be given and denote by $I = I_v^n$ and $D = D_v^n$, and $L = (K^{a,n})^D$. Assume first that there exists $I' \leq \mathbf{I}^{\text{CL}}(D') \leq \mathcal{G}_L^{a,N}$ such that $(I'_n)_K = I$ and $(D'_n)_K = D$. By Theorem 10, I is valutive, $D \leq D_{v_I}^n$ and $\text{char } k(v_I) \neq \ell$. On the other hand, $v = v_I$ by our assumption on v and I . Therefore, we see that $\text{char } k(v) \neq \ell$.

Conversely, assume that $\text{char } k(v) \neq \ell$. Then $I = T_v^n$ and $D = Z_v^n$. Chose a prolongation w of v to L and consider

$$I' := T_w^N = I_w^N \leq D_w^N = Z_w^N =: D'.$$

By Lemma 3.11 and/or Hilbert decomposition theory (see the discussion of §9), we see that $I' \leq \mathbf{I}^{\text{CL}}(D')$, as required.

Proof of (4): The proof of this is almost identical to the proof of Theorem 6 using the results of §5 instead of the results of §3 along with the discussion about Hilbert decomposition theory of §9 (see in particular the remarks at the beginning of the proof); in particular, here we use Theorem 8 instead of Theorem 3, Theorem 9 instead of Theorem 4, and Theorem 10 instead of Theorem 5. \square

11. STRUCTURE OF MAXIMAL PRO- ℓ GALOIS GROUPS

Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. As in the introduction, we denote by $\mathcal{G}_K^{M,n}$ the smallest quotient of \mathcal{G}_K for which $\mathcal{G}_L^{c,N}$ is a subquotient for all $K \subset L \subset K^{a,n}$. In other words, denote by $L^{c,N}$ the extension of L such that $\text{Gal}(L^{c,N}|L) = \mathcal{G}_L^{c,N}$; take $K^{M,n}$ to be the compositum of the fields $L^{c,N}$ as L varies over all fields such that $K \subset L \subset K^{a,n}$ then $\mathcal{G}_K^{M,n} = \text{Gal}(K^{M,n}|K)$. In particular, $\mathcal{G}_K^{M,n}$ is a characteristic quotient of \mathcal{G}_K and the assignment $\mathcal{G}_K \mapsto \mathcal{G}_K^{M,n}$ is functorial.

Corollary 11.1. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that $\text{char } K = 0$ and $\mu_{2\ell^N} \subset K$. Assume that there exists a field F such that $\ell \neq \text{char } F > 0$, $\mu_{2\ell^N} \subset F$ and $\mathcal{G}_K^{M,n} \cong \mathcal{G}_F^{M,n}$. Then for all $v \in \mathcal{V}_{K,n}$, one has $\text{char } k(v) \neq \ell$.*

Proof. Observe that for any valuation v of F , $\text{char } F = \text{char } k(v)$. This therefore follows from Theorem 2 part 3. \square

We recall that k is strongly ℓ -closed provided that for all finite extensions $k'|k$ one has $(k')^\times = (k')^{\times\ell}$. For instance, any perfect field of characteristic ℓ is strongly ℓ -closed, and all algebraically closed fields are strongly ℓ -closed.

Corollary 11.2. *Suppose that K is one of the following:*

- *A function field over a global field k of characteristic 0 such that $\mu_{2\ell} \subset k$, and $\dim(K|k) \geq 1$.*
- *A function field over a strongly ℓ -closed field k of characteristic 0 such that $\dim(K|k) \geq 2$.*

Then there does not exist a field F such that $\mu_{2\ell} \subset F$, $\text{char } F > 0$ and $\mathcal{G}_K \cong \mathcal{G}_F$.

Proof. Using Corollary 11.1, it suffices to find a valuation $v \in \mathcal{V}_{K,1}$ such that $\text{char } k(v) = \ell$. Furthermore, using the argument of Example 4.3, it suffices to find a valuation v of K such that Γ_v contains no non-trivial ℓ -divisible convex subgroups, and $k(v)$ is a function field over perfect field of characteristic ℓ . In both cases, if $\dim(K|k) \geq 2$, there exists such a valuation, taking, for example, v a quasi-prime divisor prolonging the ℓ -adic valuation of $\mathbb{Q} \subset k$ – see e.g. the Appendix of [Pop06b] and in particular Facts 5.4-5.6 and Remark 5.7 of loc.cit.. On the other hand, if $\dim(K|k) = 1$ in the first case, we can choose a model for K , $\mathcal{X} \rightarrow \text{Spec } \mathcal{O}_\ell$, where \mathcal{O}_ℓ denotes some prolongation of the ℓ -adic valuation to k ; then take v the valuation associated to some prime divisor in the special fiber of $\mathcal{X} \rightarrow \text{Spec } \mathcal{O}_\ell$. \square

Part 4. Proof of Theorem 3

APPENDIX A. PROOF OF THEOREM 3

Before we begin to prove Theorem 3, let us formalize the discussion of Remark 3.8 into a lemma which will be used in the proof.

Lemma A.1. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $M = \mathbf{M}_1(n)$. Suppose that $a, b, c, d \in R_M$ are given such that $ad = bc$. Then $\langle (a, b), (c, d) \rangle \bmod \ell^n$ is cyclic.*

In particular, let $f, g \in \mathcal{G}_K^a(M)$ be a given C-pair. Denote by $\Psi = (f_n, g_n)$. Then for all $x \notin \ker \Psi$ one has:

$$\langle \Psi(1 - x), \Psi(x) \rangle \text{ is cyclic.}$$

Proof. The $n = 1$ and $n = \infty$ case are both trivial. Thus, assume that $n \in \mathbb{N}$ is arbitrary. Assume, e.g., that $a = ec$ for some $e \in \mathbb{Z}/\ell^M$ (otherwise $c = ea$ for some $e \in \mathbb{Z}/\ell^M$). Then $ad = bc = edc$. If $c \not\equiv 0 \bmod \ell^n$ then we see that $de = b \bmod \ell^n$ by the cancelation principle; thus $(a, b) = e \cdot (c, d) \bmod \ell^n$. On the other hand, if $c \equiv 0 \bmod \ell^n$ then $a = 0 \bmod \ell^n$ as well, so that $\langle (a, b), (c, d) \rangle \bmod \ell^n = \langle (0, b), (0, d) \rangle \bmod \ell^n$ is cyclic. \square

We now proceed to prove Theorem 3. The proof will proceed in two main steps. First, we will prove the theorem for $n \in \mathbb{N}$ and then prove it for $n = \infty$ with a limit argument using the first case. Alternatively in the $n = \infty$ case, see [Top12] Theorem 3 in the “pro- ℓ case” which proves this case directly.

We briefly recall some facts from the theory of rigid element which describe the minimal conditions for the existence of valuations in fields – here we use the results of [AEJ87], but see also the various references on this subject mentioned in the introduction. For a field K , and $T \leq H \leq K^\times$, assume that $-1 \in T$ and for all $x \notin H$ one has $T + xT \subset T \cup xT$. If there exists an element $a \in K^\times \setminus T$ such that $T + aT \not\subset T \cup aT$ then there exists a valuation ring $(\mathcal{O}, \mathfrak{m})$ of K such that $1 + \mathfrak{m} \leq T$ and $\mathcal{O}^\times \leq H$ (see Proposition 2.14 of loc.cit.). On the other hand, if $H = T$, then there exists a valuation ring $(\mathcal{O}, \mathfrak{m})$ of K such that $1 + \mathfrak{m} \leq T$ and $\mathcal{O}^\times \cdot T/T$ has order at most 2 (see Theorem 2.16 and/or Corollary 2.17 of loc.cit.).

A.1. Case $n \neq \infty$. We will first prove the theorem in the case where $n \in \mathbb{N}$. We denote by $N = \mathbf{N}(n) = \mathbf{M}_1(\mathbf{N}'(n))$, $N' = \mathbf{N}'(n)$ and $M = \mathbf{M}_1(n)$ as defined in § 2. Suppose we are given $f, g \in \mathcal{G}_K^a(n)$ as well as lifts $f'', g'' \in \mathcal{G}_K^a(N)$ which form a C-pair. The goal is to show that there exists a valuation v of K such that $f, g \in D_v(n)$ and $\langle f, g \rangle / \langle f, g \rangle \cap I_v(n)$ is cyclic.

We denote by $f' = f''_{N'}$ and $g' = g''_{N'}$. Denote by $\Psi = (f, g)$ and $\Phi = (f', g')$, and consider $T = \ker \Psi$ as above. By Lemma A.1, for all $x \in K^\times$, $x \neq -1$ one has:

$$\langle \Phi(1 + x), \Phi(x) \rangle \text{ is cyclic.}$$

In particular, the same is true for Ψ . Denote by H the subgroup of K^\times generated by T and all $x \in K^\times \setminus T$ such that $1 + x \neq 1, x \bmod T$ (i.e. x such that $\Psi(1 + x) \neq \Psi(1), \Psi(x)$). Our central claim will be that H/T is cyclic.

Before we prove this claim, let us show how this would imply Theorem 3. First, if $H = T$, then for all $x \in K^\times$, such that $\Psi(x) \neq 0$ one has $\Psi(1 + x) = \Psi(1)$ or $\Psi(1 + x) = \Psi(x)$. I.e. if $x \notin T$ one has $1 + x \in T \cup xT$. By [AEJ87] Theorem 2.16 and/or Corollary 2.17 we deduce that there exists a valuation v of K such that $1 + \mathfrak{m}_v \leq T$ and $\#(\mathcal{O}_v^\times \cdot T/T) \leq 2$, thus proving our claim.

On the other hand, if $H \neq T$ then there exists some $x \notin T$ such that $\Psi(1 + x) \neq \Psi(1), \Psi(x)$ and so $1 + x \notin T \cup xT$. Moreover, for all $x \notin H$, one has $1 + x \in T \cup xT$ by construction of H . Again by [AEJ87] Proposition 2.14 (along with Observation 2.3 of loc.cit.), we deduce that there exists a valuation v of K such that $1 + \mathfrak{m}_v \leq T$ and $\mathcal{O}_v^\times \cdot T = H$.

Thus, what remains to be shown is that H/T is cyclic and this will be done in steps 1-5 below. In the case where $n = 1$, this claim can be obtained from [Koe98] Lemma 3.3, a

form of which also appears in [Koe95], and/or [Efr99] Proposition 3.2; this lemma is the key technical tool used in order to prove the main Theorem of [EK98]. On the other hand, if $n = \infty$ and K contains an ℓ -closed field, the corresponding claim can be deduced in a similar way to [BT02] Proposition 4.1.2; this proposition is in the core of the proof of loc.cit.'s main theorem. See also [Top12] Theorem 3 where the $n = \infty$ case is proved directly, without the assumption that K contains an ℓ -closed field. Below, we prove the claim for an arbitrary $n \in \mathbb{N}$.

Main Claim: H/T is cyclic.

The remainder of this section will be devoted to the proof of this claim. To make the notation a bit less cumbersome, we will use the following convention. For $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}/\ell^s$, we will write:

$$\gamma_1 : \gamma_2 = \gamma_3$$

to mean that $\gamma_1\gamma_2 = \gamma_1\gamma_3$. Also, we will write $(i, j) = (\gamma_1 : \gamma_2 : \gamma_3)$ to mean that $i \cdot \gamma_1 = \gamma_2$ and $j \cdot \gamma_1 = \gamma_3$. Furthermore, we will use the notation $(i, j) = \gamma(\gamma_1 : \gamma_2 : \gamma_3)$ to mean that $(i, j) = (\gamma\gamma_1 : \gamma\gamma_2 : \gamma\gamma_3)$.

Suppose x, y are given such that $\Psi(1+x) \neq \Psi(1), \Psi(x)$ and $\Psi(1+y) \neq \Psi(1), \Psi(y)$ and assume that $\Phi(1+x) = a\Phi(x)$ and $\Phi(1+y) = b\Phi(y)$. We will show that $\langle \Psi(x), \Psi(y) \rangle$ is cyclic for all such x, y ; this will suffice to show that H/T is cyclic as follows. Indeed, for any given $x \in K^\times \setminus T$, one has $\Psi(1-x) \neq \Psi(1), \Psi(x)$ iff $\Psi(1-(1-x)) \neq \Psi(1), \Psi(1-x)$ (also recall that $\Phi(-1) = 0$). In particular, we see that H is generated by $T = \ker(\Psi)$ and all $x \neq 0, -1$ such that $\Psi(1+x) \neq \Psi(1), \Psi(x)$ and $\Psi(1+x) \in \langle \Psi(x) \rangle$; furthermore, $\Psi(1+x) \in \langle \Psi(x) \rangle$ if and only if $\Phi(1+x) \in \langle \Phi(x) \rangle$, since $\langle \Phi(1+x), \Phi(x) \rangle$ is cyclic.

Moreover, since $\Phi(1+1/x) = \Phi(1/x) + \Phi(1+x) = (a-1)\Phi(x) = (1-a)\Phi(1/x)$, we can assume without loss that a, b are units by replacing x with $1/x$ and/or y with $1/y$ if needed. We denote by $D = f'(x)g'(y) - f'(y)g'(x)$ and take linear combinations p, q of f', g' so that:

- $(p, q)(x) = (D, 0)$ and
- $(p, q)(y) = (0, D)$.

And thus:

- $(p, q)(1+x) = (aD, 0)$ and
- $(p, q)(1+y) = (0, bD)$.

Furthermore, we will denote by $a' = a - 1$ and $b' = b - 1$. Recall that our assumptions on a, b ensure that:

- $a, a' \neq 0 \pmod{\ell^n}$.
- $b, b' \neq 0 \pmod{\ell^n}$.

To show that $\langle \Psi(x), \Psi(y) \rangle$ is cyclic, it will suffice to prove that $D = 0 \pmod{\ell^M}$ by Lemma A.1. Furthermore, we observe that p, q form a C-pair and $p(-1) = q(-1) = 0$. In particular for all $z, w \in K^\times$, $z \neq -w$, the following determinant is zero:

$$\begin{vmatrix} p(z+w) - p(w) & p(z) - p(w) \\ q(z+w) - q(w) & q(z) - q(w) \end{vmatrix} = 0.$$

Step 1: Consider $\Phi(1+x+y)$; for simplicity, denote $\Phi(1+x+y) = (P, Q)$. We can write $1+x+y = (1+x) + y$ and thus:

$$\begin{vmatrix} p(1+x+y) - p(y) & p(1+x) - p(y) \\ q(1+x+y) - q(y) & q(1+x) - q(y) \end{vmatrix} = 0.$$

Making the appropriate substitutions:

$$\begin{vmatrix} P & aD \\ Q - D & -D \end{vmatrix} = D \cdot \begin{vmatrix} P & -a \\ Q - D & 1 \end{vmatrix} = 0.$$

In other words we deduce (I) $\boxed{D : P + aQ = aD}$; similarly (II) $\boxed{D : bP + Q = bD}$ since $1 + x + y = (1 + y) + x$. Using equations (I) and (II), we deduce the following (in steps):

- (1) $D : P + a(bD - bP) = aD$
- (2) $D : P + ab(D - P) = aD$
- (3) $D : P(1 - ab) = Da(1 - b)$
- (4) $D : P(ab - 1) = Dab'$
- (5) $D : P(a'b' + a' + b') = Dab'$ and in a similar way $D : Q(a'b' + a' + b') = Da'b$.

In particular, we deduce:

$$(A.1) \quad \boxed{\Phi(1 + x + y) = D(a'b' + a' + b' : Dab' : Da'b)}.$$

Step 2: We now consider $\Phi(2 + x + y)$; for simplicity, we again denote $\Phi(2 + x + y) = (P, Q)$. Since $2 + x + y = 1 + (1 + x + y)$ one has:

$$\begin{vmatrix} p(2 + x + y) & p(1 + x + y) \\ q(2 + x + y) & q(1 + x + y) \end{vmatrix} = 0$$

Use Equation (A.1) and multiply the second column of this matrix by $D(a'b' + a' + b')$ to deduce:

$$D \begin{vmatrix} P & Dab' \\ Q & Dba' \end{vmatrix} = D^2 \begin{vmatrix} P & ab' \\ Q & ba' \end{vmatrix} = 0.$$

So that we deduce (III) $\boxed{D^2 : ba'P = ab'Q}$.

On the other hand, $2 + x + y = (1 + x) + (1 + y)$ so that:

$$\begin{vmatrix} P - p(1 + y) & p(1 + x) - p(1 + y) \\ Q - q(1 + y) & q(1 + x) - q(1 + y) \end{vmatrix} = 0$$

Making the appropriate substitutions:

$$\begin{vmatrix} P & aD \\ Q - bD & -bD \end{vmatrix} = D \cdot \begin{vmatrix} P & a \\ Q - bD & -b \end{vmatrix} = 0$$

So that we deduce (IV) $\boxed{D : bP + aQ = abD}$. Using equations (III) and (IV), we deduce the following, in steps (recall that a, b are units):

- (1) $D^2 : ba'P = b'(abD - bP)$
- (2) $D^2 : ba'P = bb'(aD - P)$
- (3) $D^2 : P(ba' + bb') = bb'aD$
- (4) $D^2 : P(a' + b') = b'aD$ and similarly $D^2 : Q(a' + b') = a'bD$.

Thus:

$$(A.2) \quad \boxed{\Phi(2 + x + y) = D^2 \cdot (a' + b' : ab'D : ba'D)}$$

Step 3 (an inductive step): Let m be a positive integer and denote by $A = D^e(a')^f(b')^g$ and $B = D^h(a')^i(b')^j$. Assume that the following statements hold:

- (P1)(\mathbf{m}, \mathbf{A}) : $\Phi((m - 1) + mx) = A \cdot (a'b' + mb' : mDab' : 0)$.
- (P2)(\mathbf{m}, \mathbf{B}) : $\Phi(m + mx + y) = B \cdot (a'b' + mb' + a' : mDab' : Da'b)$.

We will show, in particular, that the following statements hold:

- **(P1)**($\mathbf{m} + \mathbf{1}, \mathbf{E}$)
- **(P2)**($\mathbf{m} + \mathbf{1}, \mathbf{E}$)

where $E = D^{\max(2,e,h)+2}(a')^{\max(f,i)+1}(b')^{\max(g,j)+1}$ is determined by the exponents of D, a', b' in A and B . To simplify the notation, we will denote:

- $\Delta_0 = a' + b'$.
- $\Delta_1 = a'b' + mb'$.
- $\Delta_2 = a'b' + mb' + a'$.

Let us first consider $(P, Q) = \Phi((m+1) + (m+1)x + y)$, and we observe that $(m+1) + (m+1)x + y = ((m-1) + mx) + (2 + x + y)$. Thus,

$$\begin{vmatrix} P - p((m-1) + mx) & p(2 + x + y) - p((m-1) + mx) \\ Q - q((m-1) + mx) & q(2 + x + y) - q((m-1) + mx) \end{vmatrix} = 0.$$

Now by statement **(P1)**(\mathbf{m}, \mathbf{A}), we deduce that:

$$A \cdot \begin{vmatrix} \Delta_1 P - mDab' & \Delta_1 p(2 + x + y) - mDab' \\ Q & q(2 + x + y) \end{vmatrix} = 0$$

Denote by $A' = D^{\max(2,e)}(a')^f(b')^g$ then by Equation (A.2) we deduce that:

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & \Delta_1 Dab' - \Delta_0 mDab' \\ Q & Da'b \end{vmatrix} = 0.$$

Moving some terms around a bit, we have

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & Dab'(\Delta_1 - \Delta_0 m) \\ Q & Da'b \end{vmatrix} = 0$$

and now substituting into Δ_1 and Δ_0 we have:

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & Dab'(a'b' + mb' - ma' - mb') \\ Q & Da'b \end{vmatrix} = 0$$

so that

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & Dab'(a'b' - ma') \\ Q & Da'b \end{vmatrix} = 0$$

and finally

$$A'Da' \cdot \begin{vmatrix} \Delta_1 P - mDab' & ab'(b' - m) \\ Q & b \end{vmatrix} = 0.$$

Thus we obtain the following equations, by steps:

- (1) $A'Da' : b(a'b' + mb')P = Qab'(b' - m) + mDabb'$.
- (2) $A'Da' : bb'(a' + m)P = Qab'(b' - m) + mDabb'$.
- (3) (V) $\boxed{A'Da'b' : Pb(a' + m) = Qa(b' - m) + mDab}$.

On the other hand, we can write $(m+1) + (m+1)x + y = (m + mx + y) + (1 + x)$ so that:

$$\begin{vmatrix} P - p(1 + x) & p(m + mx + y) - p(1 + x) \\ Q - q(1 + x) & q(m + mx + y) - q(1 + x) \end{vmatrix} = 0.$$

Making the appropriate substitutions, we have

$$\left| \begin{array}{cc} P - aD & p(m + mx + y) - aD \\ Q & q(m + mx + y) \end{array} \right| = 0.$$

Now we use statement **(P2)**(**m, B**) to deduce that:

$$B \cdot \left| \begin{array}{cc} P - aD & mDab' - \Delta_2 aD \\ Q & Da'b \end{array} \right| = 0.$$

Rearranging a bit, we have:

$$BD \cdot \left| \begin{array}{cc} P - aD & a(mb' - \Delta_2) \\ Q & a'b \end{array} \right| = 0$$

and, substituting into Δ_2 ,

$$BD \cdot \left| \begin{array}{cc} P - aD & a(mb' - a'b' - mb' - a') \\ Q & a'b \end{array} \right| = 0$$

so that

$$BD \cdot \left| \begin{array}{cc} P - aD & -aa'(b' + 1) \\ Q & a'b \end{array} \right| = 0.$$

Now recall that $b' = b - 1$; therefore

$$BD \cdot \left| \begin{array}{cc} P - aD & -aa'b \\ Q & a'b \end{array} \right| = 0$$

and

$$BDa' \cdot \left| \begin{array}{cc} P - aD & -a \\ Q & 1 \end{array} \right| = 0.$$

Thus finally, we deduce that (VI) $\boxed{BDa' : P + aQ = aD}$. Denote by

$$C = D^{\max(2,e,h)}(a')^{\max(f,i)}(b')^{\max(g,j)}.$$

So, using equations (V) and (VI), we deduce, in steps:

- (1) $Da'b'C : Pb(a' + m) = (aD - P)(b' - m) + mDab.$
- (2) $Da'b'C : P(b(a' + m) + b' - m) = aD(b' - m) + mDab.$
- (3) $Da'b'C : P(ba' + bm + b' - m) = a(D(b' - m) + mDb).$
- (4) $Da'b'C : P(ba' + bm + b' - m) = aD(b' - m + mb).$
- (5) $Da'b'C : P(ba' + bm + b' - m) = aD(b - 1 - m + mb).$
- (6) $Da'b'C : P(ba' + bm + b' - m) = aD((m + 1)b - (m + 1)).$
- (7) (VII) $\boxed{Da'b'C : P(ba' + bm + b' - m) = (m + 1)aDb'}.$

Let us write $ba' + bm + b' - m$ in a different way:

$$\begin{aligned}
ba' + mb + b' - m &= b(a - 1) + mb + b - 1 - m \\
&= ab - b + mb + b - 1 - m \\
&= ab + mb - (m + 1) \\
a'b' + (m + 1)b' + a' &= (a - 1)(b - 1) + (m + 1)(b - 1) + a - 1 \\
&= ab - a - b + 1 + (m + 1)b - (m + 1) + a - 1 \\
&= ab + mb - (m + 1)
\end{aligned}$$

This calculation, along with equation (VII) then implies:

$$(A.3) \quad \boxed{Da'b'C : P(a'b' + (m + 1)b' + a') = (m + 1)Dab'}$$

Using euqations (A.3) and (VI), we see that:

- (1) $Da'b'C : (m + 1)Dab' + a(a'b' + (m + 1)b' + a')Q = aD(a'b' + (m + 1)b' + a')$.
- (2) $Da'b'C : a(a'b' + (m + 1)b' + a')Q = aD(a'b' + a')$.
- (3) $Da'b'C : (a'b' + (m + 1)b' + a')Q = Da'(b' + 1)$.
- (4) (VIII) $\boxed{Da'b'C : (a'b' + (m + 1)b' + a')Q = Da'b'}$.

Thus: $(\mathbf{P2})(\mathbf{m} + \mathbf{1}, \mathbf{Da'b'C})$ holds and, in particular, $(\mathbf{P2})(\mathbf{m} + \mathbf{1}, \mathbf{E})$ holds for $E = D^2a'b'C$ as above; however, we will use the stronger fact that $(\mathbf{P2})(\mathbf{m} + \mathbf{1}, \mathbf{Da'b'C})$ holds in our calculations below.

Now we consider instead $(P, Q) = \Phi(m + (m + 1)x)$. We can write $m + (m + 1)x = ((m - 1) + mx) + (1 + x)$ to deduce that:

$$\begin{vmatrix} P - p(1 + x) & p((m - 1) + mx) - p(1 + x) \\ Q - q(1 + x) & q((m - 1) + mx) - q(1 + x) \end{vmatrix} = 0.$$

Making the appropriate substitutions, we have

$$\begin{vmatrix} P - aD & p((m - 1) + mx) - aD \\ Q & q((m - 1) + mx) \end{vmatrix} = 0$$

and then using statement $(\mathbf{P1})(\mathbf{m}, \mathbf{A})$ we have:

$$A \cdot \begin{vmatrix} P - aD & mDab' - \Delta_1 aD \\ Q & 0 \end{vmatrix} = 0.$$

Factoring out a D and substituting into Δ_1 we obtain:

$$AD \cdot \begin{vmatrix} P - aD & mb' - (a'b' + mb') \\ Q & 0 \end{vmatrix} = 0$$

and so:

$$AD \cdot \begin{vmatrix} P - aD & a'b' \\ Q & 0 \end{vmatrix} = 0.$$

Thus, we have (IX) $\boxed{Q \cdot (ADa'b') = 0}$.

Let us now furthermore denote by $(P', Q') = \Phi(m + 1 + (m + 1)x + y)$, and $\Delta'_2 = a'b' + (m+1)b' + a'$, $C' = Da'b'C$. Observe that $m + (m+1)x = ((m+1) + (m+1)x + y) - (1+y)$ so that:

$$\begin{vmatrix} P - p(1+y) & P' - p(1+y) \\ Q - q(1+y) & Q' - q(1+y) \end{vmatrix} = 0$$

and making the appropriate substitutions:

$$\begin{vmatrix} P & P' \\ Q - bD & Q' - bD \end{vmatrix} = 0.$$

Now we use the fact that $(\mathbf{P2})(\mathbf{m} + \mathbf{1}, \mathbf{Da'b'C})$ (i.e. $(\mathbf{P2})(\mathbf{m} + \mathbf{1}, \mathbf{C}')$) holds to deduce that:

$$C' \cdot \begin{vmatrix} P & (m+1)Da'b' \\ Q - bD & Da'b - \Delta'_2 bD \end{vmatrix} = 0$$

and so

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ Q - bD & a'b - \Delta'_2 b \end{vmatrix} = 0.$$

Now, we observe that $ADa'b'|C'D$ so that equation (IX) above implies that:

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ -bD & a'b - \Delta'_2 b \end{vmatrix} = 0$$

and, since b is a unit, we obtain

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ -D & a' - \Delta'_2 \end{vmatrix} = 0.$$

Now we substitute into Δ_2 to obtain:

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ -D & a' - (a'b' + (m+1)b' + a') \end{vmatrix} = 0.$$

Thus we have

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ D & a'b' + (m+1)b' \end{vmatrix} = 0.$$

In particular, we obtain the following equation:

$$\boxed{E = C'D : P(a'b' + (m+1)b') = (m+1)Da'b'}.$$

Therefore the statements $(\mathbf{P1})(\mathbf{m} + \mathbf{1}, \mathbf{D^2a'b'C})$, $(\mathbf{P2})(\mathbf{m} + \mathbf{1}, \mathbf{Da'b'C})$ hold. Recall that $C = D^{\max(2,e,h)}(a')^{\max(f,i)}(b')^{\max(g,j)}$. Thus, denoting by

$$E = D^{\max(2,e,h)+2}(a')^{\max(f,i)+1}(b')^{\max(g,j)+1},$$

we then deduce that the following statements hold:

$$(\mathbf{P1})(\mathbf{m} + \mathbf{1}, \mathbf{E}), \quad (\mathbf{P2})(\mathbf{m} + \mathbf{1}, \mathbf{E})$$

as contended.

Step 4 (calculating $\Phi((m-1) + mx)$): Our base case is $m = 1$. Indeed, observe that $\Phi(x) = (D, 0) = (a'b' + b' : Da'b' : 0)$ (since $a' = a - 1$) and from Step 1 (see Equation (A.1)):

$$\Phi(1 + x + y) = D(a'b' + a' + b' : Da'b' : Da'b).$$

Namely, the statements $(\mathbf{P1})(\mathbf{1}, \mathbf{1})$ and $(\mathbf{P2})(\mathbf{1}, \mathbf{D})$ hold true. Thus by the inductive step (Step 3) we obtain that $(\mathbf{P1})(\mathbf{2}, \mathbf{D^4a'b'})$ and $(\mathbf{P2})(\mathbf{D^4a'b'})$ are true as well. From this we

deduce that the statements $(\mathbf{P1})(\mathbf{3}, \mathbf{D}^6(\mathbf{a}')^2(\mathbf{b}')^2)$ and $(\mathbf{P2})(\mathbf{3}, \mathbf{D}^6(\mathbf{a}')^2(\mathbf{b}')^2)$ are true. We deduce inductively that, in general, the following statements hold:

$$(\mathbf{P1})(\mathbf{m}, \mathbf{D}^{2\mathbf{m}}(\mathbf{a}')^{\mathbf{m}-1}(\mathbf{b}')^{\mathbf{m}-1}), (\mathbf{P2})(\mathbf{m}, \mathbf{D}^{2\mathbf{m}}(\mathbf{a}')^{\mathbf{m}-1}(\mathbf{b}')^{\mathbf{m}-1}).$$

And in particular we deduce that, for any $m \geq 1$, there exists $P_m \in \mathbb{Z}/\ell^{N'}$ such that the following equation holds:

$$D^{2m}(a')^{m-1}(b')^{m-1} : (a'b' + mb') \cdot P_m = Dmab'$$

Alternatively:

$$D^{2m}(a')^{m-1}(b')^m : (a' + m) \cdot P_m = Dma.$$

This means that the following equation holds for the elements $P_m, D, a', b', m, a, b \in \mathbb{Z}/\ell^{N'}$:

$$(A.4) \quad \boxed{D^{2m}(a')^{m-1}(b')^m \cdot Dma = D^{2m}(a')^{m-1}(b')^m \cdot (a' + m) \cdot P_m.}$$

Step 5 (Deduce that $D = 0 \pmod{\ell^M}$): For non-zero elements $\eta \in \mathbb{Z}/\ell^s$ we will denote by $\mathbf{o}(\eta) = \text{ord}_\ell(\tilde{\eta})$ where $\tilde{\eta}$ denotes some lift of η to \mathbb{Z}_ℓ ; we observe that $\mathbf{o}(rt) = \mathbf{o}(r) + \mathbf{o}(t)$ if $r, t, rt \neq 0 \pmod{\ell^s}$.

Assume, for a contradiction, that $D \neq 0 \pmod{\ell^M}$ so that $\mathbf{o}(D) \leq M - 1 = 2(n - 1)$. Take $1 \leq m \leq \ell^{3n-2} - 1$ to be a representative for $-a' \pmod{\ell^{3n-2}}$ and thus, in particular, $\mathbf{o}(m) \leq n - 1$. Observe that

$$N' = (6\ell^{3n-2} - 7)(n - 1) + 3n - 2 \geq (6m - 1)(n - 1) + 3n - 2.$$

Let us now consider the orders of the elements in the left-hand-side of Equation (A.4). Since $\mathbf{o}(D) \leq 2n - 2$ and $\mathbf{o}(a'), \mathbf{o}(b'), \mathbf{o}(m) \leq n - 1$ we deduce that:

$$2m\mathbf{o}(D) + (m - 1)\mathbf{o}(a') + m\mathbf{o}(b') + \mathbf{o}(D) + \mathbf{o}(m) + 1 \leq (6m - 1)(n - 1) + 3n - 2$$

Moreover, we recall that $\mathbf{o}(a) = 0$. Thus left-hand-side of equation (A.4) is non-zero as an element of $\mathbb{Z}/\ell^{N'}$. We deduce, in particular, that $\mathbf{o}(D) + \mathbf{o}(m) = \mathbf{o}(a' + m) + \mathbf{o}(P_m)$ by Equation (A.4). However, $a' + m = 0 \pmod{\ell^{3n-2}}$ so that:

$$3n - 3 \geq \mathbf{o}(D) + \mathbf{o}(m) = \mathbf{o}(a' + m) + \mathbf{o}(P_m) \geq 3n - 2$$

and this is a contradiction.

We therefore obtain that $D = 0 \pmod{\ell^M}$, as required. Using the discussion preceeding Step 1 above, this then implies the Main Claim. And thus, finally, we've proven Theorem 3 for $n \in \mathbb{N}$.

A.2. Case $n = \infty$. Let us now show how to deduce the theorem for $n = \infty$; this will follow from a limit argument using the $n \in \mathbb{N}$ case proved above.

Let $f, g \in \mathcal{G}_K^a(\infty)$ be a given C-pair. Equivalently, f_n, g_n form a C-pair for all $n \in \mathbb{N}$. Consider, then:

$$T := \ker f \cap \ker g, \quad T_n := \ker f_n \cap \ker g_n.$$

Then $T_n \geq T_{n+1}$ and $T = \bigcap_n T_n$. Denote by $\Psi = (f, g)$ and $\Psi_n = (f_n, g_n)$. Denote by H the subgroup generated by T and all $x \notin T$ such that $\Psi(1+x) \neq \Psi(1), \Psi(x)$. Arguing as in the previous case, it suffices to show that $\text{Hom}(K^\times/T, \mathbb{Z}_\ell)/\text{Hom}(K^\times/H, \mathbb{Z}_\ell)$ is cyclic. And in order to show this it suffices to prove that $(T_n \cdot H)/T_n$ is cyclic for all $n \in \mathbb{N}$.

For each $n \in \mathbb{N}$ denote by H_n the subgroup generated by T_n and all $x \notin T_n$ such that $\Psi_n(1+x) \neq \Psi_n(1), \Psi_n(x)$. Furthermore, if $\Psi_n(x) \neq 0$ and $\Psi_n(1+x) \neq \Psi_n(1), \Psi_n(x)$ then also $\Psi_N(x) \neq 0$ and $\Psi_N(1+x) \neq \Psi_N(1), \Psi_N(x)$ for all $N \geq n$. Thus, $H_n \leq T_n \cdot H_N$ and so

$H_n/T_n \leq (T_n \cdot H_N)/T_n$. Therefore $(T_n \cdot H)/T_n = \bigcup_{N \geq n} (T_n \cdot H_N)/T_n$ is an inductive union. By the first case, H_N/T_N is always cyclic (for all N) and thus $(T_n \cdot H_N)/T_n$ is cyclic for all $N \geq n$. Therefore, $(T_n \cdot H)/T_n$ is cyclic, as required.

REFERENCES

- [AEJ87] J. Arason, R. Elman, and B. Jacob, *Rigid elements, valuations, and realization of Witt rings*, J. Algebra **110** (1987), no. 2, 449–467. MR910395 (89a:11041) ↑[3](#), [10](#), [38](#)
- [Bog91] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, Algebraic geometry and analytic geometry (Tokyo, 1990), 1991, pp. 26–52. MR1260938 (94k:14013) ↑[2](#), [4](#)
- [BT02] F. A. Bogomolov and Y. Tschinkel, *Commuting elements of Galois groups of function fields*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), 2002, pp. 75–120. ↑[2](#), [3](#), [4](#), [6](#), [9](#), [10](#), [13](#), [39](#)
- [BT08] ———, *Reconstruction of function fields*, Geom. Funct. Anal. **18** (2008), no. 2, 400–462. MR2421544 (2009g:11155) ↑[2](#), [4](#)
- [Efr06] I. Efrat, *Quotients of Milnor K -rings, orderings, and valuations*, Pacific J. Math. **226** (2006), no. 2, 259–275. MR2247864 (2007h:19004) ↑[24](#)
- [Efr07] ———, *Compatible valuations and generalized Milnor K -theory*, Trans. Amer. Math. Soc. **359** (2007), no. 10, 4695–4709 (electronic). MR2320647 (2008g:19004) ↑[3](#), [24](#)
- [Efr95] ———, *Abelian subgroups of pro-2 Galois groups*, Proc. Amer. Math. Soc. **123** (1995), no. 4, 1031–1035. MR1242081 (95e:12007) ↑[1](#), [3](#), [6](#)
- [Efr98] ———, *Small maximal pro- p Galois groups*, Manuscripta Math. **95** (1998), no. 2, 237–249. MR1603329 (99e:12005) ↑[1](#)
- [Efr99] ———, *Construction of valuations from K -theory*, Math. Res. Lett. **6** (1999), no. 3-4, 335–343. MR1713134 (2001i:12011) ↑[3](#), [39](#)
- [EK98] A. J. Engler and J. Koenigsmann, *Abelian subgroups of pro- p Galois groups*, Trans. Amer. Math. Soc. **350** (1998), no. 6, 2473–2485. MR1451599 (98h:12004) ↑[1](#), [3](#), [6](#), [39](#)
- [EM11a] I. Efrat and J. Mináč, *Small Galois groups that encode valuations*, Acta Arithmetica (to appear) (May 2011), available at [arXiv:1105.2427](#). ↑[2](#), [6](#)
- [EM11b] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups*, American Journal of Mathematics **133** (2011), no. 6, 1503–1532, available at [arXiv:0809.2166](#). ↑[29](#)
- [EN94] A. J. Engler and J. B. Nogueira, *Maximal abelian normal subgroups of Galois pro-2-groups*, J. Algebra **166** (1994), no. 3, 481–505. MR1280589 (95h:12004) ↑[1](#), [3](#), [6](#)
- [Koe01] J. Koenigsmann, *Solvable absolute Galois groups are metabelian*, Invent. Math. **144** (2001), no. 1, 1–22. MR1821143 (2002a:12006) ↑[1](#)
- [Koe95] ———, *From p -rigid elements to valuations (with a Galois-characterization of p -adic fields)*, J. Reine Angew. Math. **465** (1995), 165–182. With an appendix by Florian Pop. MR1344135 (96m:12003) ↑[3](#), [39](#)
- [Koe98] ———, *Pro- p Galois groups of rank ≤ 4* , Manuscripta Math. **95** (1998), no. 2, 251–271. MR1603333 (99e:12004) ↑[1](#), [38](#)
- [MMS04] L. Mahé, J. Mináč, and T. L. Smith, *Additive structure of multiplicative subgroups of fields and Galois theory*, Doc. Math. **9** (2004), 301–355. MR2117418 (2006b:11040) ↑[2](#)
- [Neu69a] J. Neukirch, *Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen*, J. Reine Angew. Math. **238** (1969), 135–147. MR0258804 (41 #3450) ↑[1](#)
- [Neu69b] ———, *Kennzeichnung der p -adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 296–314. MR0244211 (39 #5528) ↑[1](#)
- [NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Second, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2008. MR2392026 (2008m:11223) ↑[27](#), [28](#)
- [Pop00] F. Pop, *Alterations and birational anabelian geometry*, Resolution of singularities (Obergrugl, 1997), 2000, pp. 519–532. MR1748633 (2001g:11171) ↑[1](#)

- [Pop06a] ———, *Almost commuting elements in small Galois groups*, 2006. In Oberwolfach Report 25/2006, Mathematisches Forschungsinstitut Oberwolfach, Pro-p Extensions of Global Fields and pro-p Groups, May 21-27 2006, pg. 1495-1496. [↑2](#)
- [Pop06b] ———, *Galois theory of Zariski prime divisors*, Groupes de Galois arithmétiques et différentiels, 2006, pp. 293–312. MR2316355 (2008d:12006) [↑37](#)
- [Pop10a] ———, *On the birational p -adic section conjecture*, Compos. Math. **146** (2010), no. 3, 621–637. MR2644930 (2011d:14045) [↑35](#)
- [Pop10b] ———, *Pro- ℓ abelian-by-central Galois theory of prime divisors*, Israel J. Math. **180** (2010), 43–68. MR2735055 (2012a:12010) [↑2](#), [3](#), [4](#), [34](#)
- [Pop12a] ———, *\mathbb{Z}/ℓ abelian-by-central Galois theory of prime divisors*, The arithmetic of fundamental groups: Pia 2010, 2012, pp. 225–244. [↑34](#)
- [Pop12b] ———, *On the birational anabelian program initiated by Bogomolov I*, Invent. Math. **187** (2012), no. 3, 511–533. MR2891876 [↑2](#), [4](#)
- [Pop94] ———, *On Grothendieck’s conjecture of birational anabelian geometry*, Ann. of Math. (2) **139** (1994), no. 1, 145–182. MR1259367 (94m:12007) [↑1](#)
- [Top12] A. Topaz, *Almost-commuting-liftable subgroups of Galois groups*, Preprint (2012), available at [arXiv:1202.1786](#). [↑5](#), [6](#), [13](#), [25](#), [38](#), [39](#)
- [Uch76] K. Uchida, *Isomorphisms of Galois groups*, J. Math. Soc. Japan **28** (1976), no. 4, 617–620. MR0432593 (55 #5580) [↑1](#)
- [War81] R. Ware, *Valuation rings and rigid elements in fields*, Canad. J. Math. **33** (1981), no. 6, 1338–1355. MR645230 (83i:10028) [↑3](#)

DEPARTMENT OF MATHEMATICS,
 UNIVERSITY OF PENNSYLVANIA,
 209 S. 33RD STREET,
 PHILADELPHIA, PA 19104
E-mail address: atopaz@math.upenn.edu
URL: www.math.upenn.edu/~atopaz